# Double-Edged Sword: An Empirical Study on the Contribution of Cloud Providers in Malicious Infrastructure

Sousan Tarahomi*, Raffaele Sommese*, Jeroen Linssen‡, Ralph Holz*†, Anna Sperotto*
*University of Twente, Enschede, The Netherlands, †University of Münster, Münster, Germany
‡Saxion University of Applied Sciences, Enschede, The Netherlands
{s.tarahomi, r.sommese, r.holz, a.sperotto }@utwente.nl, j.m.linssen@saxion.nl

***Abstract*—Cloud computing offers flexibility and cost-effectiveness, but can also be abused for malicious activities. In this study, we conduct an empirical analysis of the cloud infrastructure of malicious (blocklisted) domains, with a focus on three core infrastructural components — web hosting, DNS, and email — and we compare them against a baseline of general domains. Our goal is to assess the rate of abuse targeting these components as they represent fundamental pillars of Internet communication. Leveraging DNS data from OpenINTEL, cloud classification from IP2Location, and a curated ground-truth list of cloud providers, we evaluate the role of major providers in hosting malicious infrastructure. Our results show that malicious domains are increasingly shifting toward partial cloud infrastructure outsourcing, with a strong preference for cloud-based web hosting while avoiding full-stack cloud adoption. We also observe a high degree of diversity of malicious infrastructure deployment across all three components. Finally, our country analysis highlights a growing concentration of malicious hosting activity in the Asia-Pacific region.**

## I. Introduction

Cloud technology has grown rapidly, potentially reducing costs and easing processes, but it also acts as a double-edged sword: all the features that benefit legitimate users can also be exploited by attackers to facilitate malicious activities. This growing trend of mixed use of cloud technology has reshaped both the security profile and management practices.

In the past, adversaries typically relied on either their own infrastructure or compromised systems to conduct attacks. Both approaches had their limitations: using their own infrastructure increased the risk of identification and takedown, while relying on compromised machines could be detected and patched, making the latter approach less reliable for attackers [21].

Cloud service abuse has existed since the early days of cloud adoption. In 2009, security researchers discovered a Zeus botnet controller operating on an Amazon Elastic Compute Cloud (EC2) virtual machine [6]. A recent abuse case in September 2024 revealed that the BianLian and Rhysida ransomware groups had started using Azure Storage Explorer to exfiltrate data from their victims, replacing older tools [24].

The focus of this work is assessing the rate of abuse targeting three fundamental infrastructural components of cloud, namely web hosting, DNS, and email. For this purpose, we leverage data from our active DNS measurement platform OpenINTEL [30], the geolocation dataset IP2Location [5] and several lists of blocked domains collected from various blocklist providers.

Our findings show a growing trend of partial cloud migration among malicious domains, particularly for web hosting.

This paper is organized as follows. In Sec. II, we provide an overview of the literature investigating the role of cloud providers in malicious infrastructure. Sec. III outlines our methodology, followed by a presentation of the results in Sec. IV. Sec. V highlights the limitations of our study. Finally, Sec. VI summarizes our key findings and operational considerations.

## II. Related work

Several studies have investigated abuse of Internet resources, particularly cloud services. Allegretta et al. [19] analyzed malware abuse patterns across Internet services and showed that attackers often exploit Internet service providers' domains to evade detection. We also investigate the abuse rate, specifically focusing on historical cloud-hosted infrastructure adoption. Yazdani et al. [31] studied the role of open DNS resolvers in DDoS attacks and found their concentration in some countries and operators, but diversity in network types. Similarly, we examine the concentration of blocklisted domains across countries and ASNs. Zhao et al. [32] reported that a significant portion of various malicious activities originated from the cloud by developing a machine learning model trained on blacklist data [32]. Authors in [27] used two malicious data sources (a blocklist of IPs/URLs and malicious network traces) and found cloud prefixes appear 2 to 100 times more often than non-cloud in malicious datasets. We broaden

978-3-903176-75-1 ©2025 IFIP

this work by examining additional components of the cloud ecosystem. Another study showed Bulletproof Hosting increasingly relies on lower-tier providers such as ISPs, cloud platforms, and content delivery networks (CDN) rather than centralized infrastructure, with cloud services as the main source [20]. Liao et al. [22] showed that adversaries abuse cloud repositories for web-based attacks like phishing and malware delivery, and in a similar research, the authors studied the first major keylogger that used a cloud service, Pastebin, to store stolen data [21]. While these studies provide valuable insights into the abuse of cloud infrastructure, the rapid growth of cloud services calls for further research.

## III. Methodology

We aim at detecting the contribution of cloud services in providing malicious infrastructure, with a focus on the leading providers in the cloud market. Our analysis investigates three infrastructural components: web hosting, DNS and email services, and integrates blocklisted domains, DNS measurements, and cloud IP ranges to identify cloud infrastructure used by malicious domains. By analyzing these components, we measure the extent to which cloud infrastructures are leveraged for malicious purposes compared to the baseline of general domains.

*1) Datasets:* We collected blocklisted domains on 2025-01-27 and 2021-01-27 from the following sources: DBL [9], Phishtank [14], Phishingarmy [13], Cybercrimetracker [7], Tolouse DDoS, Crypto, and Malware [16], Digitalside [8], Openphish [10], Vxvault [17], Ponmocup [11], Quidsup [15].

These blocklists are widely used in security research and cover a variety of malicious activities, such as phishing and malware. For DNS data, we used OpenINTEL [30], and cloud classification relied on IP2Location [5] and published IP ranges of major providers (AWS [1], Azure [2], Oracle [12], Google [4], DigitalOcean [3]), selected for their popularity and public availability of IP ranges. We focus on the *.com* top-level domain (TLD), which represents 38% of the DNS namespace [18] and is inexpensive to register, making it attractive to malicious actors. We analyze A, NS, and MX records of these domains to assess whether attackers utilize the cloud not only for hosting but also for DNS and email services, thereby reducing exposure and blending with benign infrastructure.

*2) The process:* We selected data from the aforementioned dates of blocklisted *.com* second-level domains (SLDs) and extracted their corresponding DNS data and IP addresses from OpenINTEL [30], and classified IP addresses into cloud and non-cloud categories, following a similar approach to [29]. Specifically, we labeled as *cloud* any IP addresses that either (i) have a usage type of *DCH* (Data Center/Web Hosting/Transit) or *CDN* (Content delivery network) in the IP2Location [5] dataset, or (ii) fall within the published IP ranges of major cloud providers mentioned in Sec. III-1. All remaining IPs were classified as *non-cloud*.

To evaluate the potential maliciousness of each infrastructural component, we compared the share of cloud infrastructure in the baseline, which includes all *.com* domains against those in blocklisted domains.

Since our blocklist contains only domain names, we joined it with historical A records from OpenINTEL to extract IPs, considering only APEX records (e.g., `example.com`) and matching them against the aforementioned cloud IP ranges to identify cloud-hosted domains. For NS and MX, we employed the same approach: extracting server IPs from OpenINTEL and mapping them to cloud IP ranges to identify blocklisted domains whose names or mail servers are cloud-hosted.

In the remainder of the paper, we use A, NS, and MX records interchangeably with web hosting, DNS, and email, respectively.

## IV. Results

In this section, we present the results of our investigation from multiple perspectives. In the Sec. IV-A, we conduct a comparative analysis of web hosting, DNS, and email in the baseline and blocklisted domains. Sec. IV-B explores the distribution of infrastructural components (A, NS, and MX records) across cloud providers. In Sec. IV-C, we focus on the contribution of major cloud providers to malicious infrastructure. Finally, we compare the cloud migration rate with a longitudinal analysis in Sec. IV-D.

### A. Comparative analysis of hosting, DNS, and email infrastructure

We first investigate the distribution of the infrastructure of blocklisted domains across countries and Autonomous System Numbers (ASN), and compare it with the baseline. Our goal is to understand which countries and ASNs most frequently host domain infrastructure, both in the baseline and blocked domains. Furthermore, we want to identify possible concentration patterns and prominent players in three infrastructural components.

*1) Frequent countries and ASNs:* Table I shows the top five countries/ASNs ranked by the number of domains whose associated infrastructure is hosted in those countries (*i.e.,* where the servers are located) or ASNs, along with the proportion of such domains relative to the total domains in the corresponding dataset. Given that a domain may have its infrastructure hosted in several countries or ASNs (*e.g.,* a domain with multiple A records in which their corresponding IPs are hosted by different countries or ASNs), we consider the total

number of distinct domains per country or ASN in our calculation. Furthermore, we define the *ratio* for a given country $c$ or ASN as:

$$\text{Ratio}(c|asn) = \frac{\text{Count}(c|asn)}{N} \quad (1)$$

where $\text{Count}(c|asn)$ is the number of domains associated with a country $c$ or an ASN $asn$ , and $N$ is the total number of unique domains in the dataset. We calculate such a ratio for both the baseline and blocked domains.

Predictably, the USA dominates all other countries with a significant difference in all three infrastructural components for both blocked domains and the baseline.

For web hosting (A) in the baseline, the infrastructure is distributed among European countries and Canada after the USA. East Asian countries such as Hong Kong, Japan, and Korea showed up at the top for blocked domains hosting infrastructure, while they are not very prevalent in the baseline.

For DNS (NS), there is a similar pattern to web hosting: we have East Asian countries like China and Japan in the top five countries in blocked domains infrastructure. In addition to them, Singapore is also among the top ones, which also shows a potential preference towards Asia-Pacific for name server hosting blocked domains. For the baseline infrastructure, there is also China, besides the European countries and Canada, among the top-listed countries.

The main distribution of mail server (MX) infrastructure for both blocked and the baseline domains is dominated by the USA and distributed across various European countries.

Most top ASNs are also US-based. Interestingly, GoDaddy's name servers are far less involved in blocked domains than in the baseline, likely due to the many parking domains it manages [33]. By contrast, Cloudflare, which also offers a free hosting plan, is more prevalent in blocked domains.

*2) Global Distribution:* Next, we measure how likely a country or ASN is to host blocked domains relative to the baseline. We aim to find countries or networks that are particularly associated with malicious activity, even if their overall volume of domains is low. For this, we introduce a metric defined as the ratio of a country's/ASN's share in blocked domains to its share in the baseline:

$$\text{Ratio}(c|asn)_{\text{blk/baseline}} = \frac{\text{Ratio}(c|asn)_{\text{blk}}}{\text{Ratio}(c|asn)_{\text{baseline}}} \quad (2)$$

Due to the high dispersion of $\text{Ratio}(c|asn)_{\text{blk/baseline}}$, we excluded countries with fewer than 10,000 occurrences in the baseline for clearer visualization. Fig. 1 shows the log-scale distribution across countries for web, DNS, and email infrastructure. Darker shading indicates a higher likelihood of hosting blocked domains, with Russia and China standing out across all components. Overall, the distribution patterns are similar across components, differing mainly in intensity.

*3) Distributional patterns in malicious infrastructure:* The proportion of malicious infrastructure in a country or ASN shows only one side of the coin. Small countries or ASNs may be over-represented due to extensive abuse of their limited infrastructure, yet their overall impact on the Internet remains low. To access the correlation between malicious usage and the baseline, we calculate the Pearson correlation between $\text{Ratio}(c|asn)_{\text{baseline}}$ and $\text{Ratio}(c|asn)_{\text{blk}}$ across all three infrastructural components. We found a strong correlation at the country-level in NS (0.99) and MX (0.98), indicating that the countries hosting name and mail servers for blocked domains largely mirror general hosting patterns. In contrast, the lower correlation for A records(0.66) suggests that blocked domains often rely on alternative web hosting locations. This pattern points to differences in web hosting choices compared to the name or mail servers, though the exact reasons remain unclear. We speculate that malicious actors may prefer generally available out-of-the-box services provided by their registry or cheap/free cloud to host their mail/name servers, as they do not consider them, with the exception of malicious mail-related activities, a primary element of their abusive activity. At the ASN level, correlations are weaker (0.27, 0.69, and 0.57 for A, NS, and MX), implying that some smaller ASNs are disproportionately attractive to malicious actors.

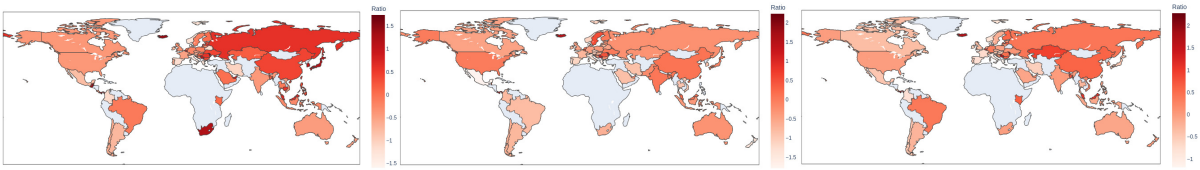
### *B. Multidimensional analysis*

To analyze how domain infrastructure is distributed across cloud providers, we conducted a multidimensional analysis on both the baseline and blocked domains. Table II shows the distribution of domains by cloud-hosted infrastructure components (A, NS, MX). Each row represents a unique combination of components and the number and percentage of associated domains. For each domain, if at least one of its corresponding infrastructure IPs, such as a name server (NS) record, is hosted in the cloud, we label the corresponding field (e.g., NS) as `True`. If none of the corresponding infrastructure IPs is in the cloud, the record name is set to `False`. Domains without infrastructure data (*e.g.,* lacking A/NS/MX records) are labeled "–". Note that a responsive domain may still lack an NS record due to mismatches between parent and child zones [26]. Since OpenINTEL queries NS records directly from child zones, such misconfigurations can be observed.

As shown in Table II, a significant proportion of domains in the baseline utilize cloud-hosted services for their entire core infrastructure stack (34.67%). To have a better representation of how often domains fully rely on cloud for their infrastructure or on a combination of

TABLE I: Top five countries and ASNs per three infrastructural components (baseline vs blocked domains)

| | | Country | # | % | ASN | Name | # | % |
|---|---|---|---|---|---|---|---|---|
| A | Baseline | United States of America | 92,010,616 | 71.33 | 16,509 | AMAZON-02 | 41,979,307 | 32.55 |
| | | Germany | 7,031,420 | 5.45 | 13,335 | CLOUDFLARENET | 11,880,143 | 9.21 |
| | | Canada | 4,641,146 | 3.60 | 53,831 | SQUARESPACE | 5,171,463 | 4.01 |
| | | Netherlands (Kingdom of the) | 3,013,850 | 2.33 | 58,182 | wix_com | 5,146,915 | 4.00 |
| | | France | 2,758,343 | 2.14 | 14,618 | AMAZON-AES | 4,594,826 | 3.56 |
| | BLK | United States of America | 225,746 | 40.11 | 152,194 | CTGSERVERLIMITED-AS-AP | 99,707 | 17.71 |
| | | Hong Kong | 189,488 | 33.66 | 13,335 | CLOUDFLARENET | 68,186 | 12.11 |
| | | Japan | 73,010 | 12.97 | 16,509 | AMAZON-02 | 38,854 | 6.90 |
| | | Germany | 27,647 | 4.91 | 40,065 | CNSERVERS | 33,050 | 5.87 |
| | | Korea (the Republic of) | 22,627 | 4.02 | 8,075 | MICROSOFT-CORP-MSN-AS-BLOCK | 20,111 | 3.57 |
| NS | Baseline | United States of America | 104,767,148 | 79.47 | 44,273 | GODADDY-DNS | 42,092,796 | 31.92 |
| | | Germany | 8,312,847 | 6.30 | 13,335 | CLOUDFLARENET | 21,745,790 | 16.50 |
| | | China | 5,660,768 | 4.29 | 15,169 | GOOGLE | 11,818,594 | 8.97 |
| | | France | 3,038,837 | 2.30 | 16,509 | AMAZON-02 | 7,765,053 | 5.89 |
| | | Canada | 3,030,299 | 2.30 | 397,213 | SECURITYSERVICES | 6,109,952 | 4.63 |
| | BLK | United States of America | 374,864 | 77.45 | 13,335 | CLOUDFLARENET | 185,447 | 38.31 |
| | | China | 102,688 | 21.21 | 16,509 | AMAZON-02 | 50,189 | 10.37 |
| | | Singapore | 64,374 | 13.30 | 8,796 | FD-298-8796 | 49,438 | 10.21 |
| | | Japan | 29,806 | 6.16 | 134,763 | CT-DongGuan-IDC | 49,163 | 10.16 |
| | | Germany | 19,526 | 4.03 | 4,837 | CHINA169-Backbone | 38,685 | 8.00 |
| MX | Baseline | United States of America | 36,947,145 | 54.88 | 15,169 | GOOGLE | 10,745,306 | 15.96 |
| | | Netherlands (Kingdom of the) | 13,491,516 | 20.04 | 21,499 | GODADDY-SXB | 7,450,851 | 11.06 |
| | | France | 9,830,905 | 14.60 | 8,075 | MICROSOFT-CORP-MSN-AS-BLOCK | 6,621,346 | 9.84 |
| | | Germany | 5,515,748 | 8.19 | 22,612 | NAMECHEAP-NET | 4,661,645 | 6.93 |
| | | Canada | 2,802,372 | 4.16 | 8,560 | IONOS-AS | 3,354,339 | 4.98 |
| | BLK | United States of America | 77,912 | 55.73 | 14,061 | DIGITALOCEAN-ASN | 21,500 | 15.38 |
| | | Netherlands (Kingdom of the) | 19,816 | 14.17 | 46,606 | UNIFIEDLAYER-AS-1 | 9,177 | 6.56 |
| | | Germany | 17,273 | 12.36 | 24,940 | HETZNER-AS | 7,500 | 5.36 |
| | | Belgium | 5,813 | 4.15 | 22,612 | NAMECHEAP-NET | 7,209 | 5.16 |
| | | France | 3,936 | 2.81 | 15,169 | GOOGLE | 7,208 | 5.16 |



(a) A (b) NS (c) MX

Fig. 1: World map of country Ratio$(c)_{\text{blk/baseline}}$ for the three infrastructure components on the logarithmic scale

TABLE II: Distribution of baseline vs. blocked domains by cloud-hosted infrastructure components.

| A | NS | MX | #Base | %Base | #Blk | %Blk |
|---|---|---|---|---|---|---|
| True | True | True | 61,832,091 | 34.67% | 113,170 | 15.78% |
| True | True | – | 55,798,500 | 31.29% | 250,425 | 34.93% |
| True | – | – | 8,928,496 | 5.01% | 187,255 | 26.11% |
| – | True | – | 6,534,882 | 3.66% | 80,815 | 11.27% |
| – | True | True | 3,711,090 | 2.08% | 14,503 | 2.02% |
| True | True | False | 1,297,645 | 0.73% | 1,058 | 0.15% |
| False | True | – | 1,165,576 | 0.65% | 17,318 | 2.41% |
| False | True | True | 792,808 | 0.44% | 1,143 | 0.16% |
| False | – | – | 582,792 | 0.33% | 5,437 | 0.76% |
| False | True | False | 575,394 | 0.32% | 2,085 | 0.29% |
| False | False | False | 507,434 | 0.28% | 2,085 | 0.29% |
| True | False | True | 478,984 | 0.27% | 151 | 0.02% |
| True | – | True | 280,659 | 0.16% | 10,549 | 1.47% |
| False | False | – | 266,607 | 0.15% | 122 | 0.02% |
| True | False | – | 264,865 | 0.15% | 125 | 0.02% |
| – | False | – | 158,732 | 0.09% | 81 | 0.01% |
| – | True | False | 122,225 | 0.07% | 5,437 | 0.76% |
| False | False | True | 103,180 | 0.06% | 159 | 0.02% |
| True | False | False | 92,048 | 0.05% | 49 | 0.01% |
| – | False | True | 78,542 | 0.04% | 17 | 0.00% |
| – | False | False | 75,714 | 0.04% | 32 | 0.00% |
| False | – | False | 44,157 | 0.02% | 37 | 0.01% |
| – | – | True | 27,481 | 0.02% | 100 | 0.01% |
| False | – | True | 11,218 | 0.01% | 8 | 0.00% |
| True | – | False | 9,357 | 0.01% | 23 | 0.00% |
| – | – | False | 7,351 | 0.00% | 37 | 0.01% |
| **Total** | | | 178,330,232 | | 717,106 | |

cloud and non-cloud infrastructure, we visualize those combinations in UpSet plots. Fig. 2c and Fig. 2d show the infrastructure distribution across the baseline and blocked domains, respectively. For simplicity and clarity in these plots, we set cases of missing records (reported as "–" in Table II) as `False`. Each bar in the upper plot represents an intersection of infrastructural categories (e.g., domains that have both A and NS records hosted on cloud providers). The lower matrix shows which record types are included in each intersection, and the percentage values reflect the proportion of total domains that fall into each category.

The overall presence of cloud-hosted infrastructure components is lower among blocked domains compared to the baseline. A significant difference is observed in domains that have only A records (web hosting infrastructure) in the cloud: while only 6.5% of the baseline fall into this category, the proportion is 26.4% for blocked domains, indicating that malicious actors largely use the cloud for hosting their web content. A notable disparity appears when all the components (A, NS, and MX records) are hosted in the cloud. This configuration is the most common among domains in baseline, representing 43.0%, whereas it ranks third among blocked domains, with a smaller share of 16.0%. Moreover, blocked domains exhibit a higher prevalence of cloud-hosted NS

records only (14.6%) compared to the domains in the baseline (5.8%), suggesting a tendency among malicious actors to selectively offload certain components to the cloud. Overall, these trends suggest that blocked domains more often rely on partial cloud infrastructure, possibly to evade detection or reduce costs, rather than fully cloud-hosted setups.

### C. Malicious activity across major cloud providers

In this section, we compare the contribution of five major cloud providers – Amazon AWS, Azure, Oracle, Google, and DigitalOcean – against other cloud providers across the three infrastructure components. This analysis shows whether malicious infrastructure is concentrated among cloud market leaders or more broadly distributed, and identifies which major provider contributes more to malicious infrastructure. This helps us to spot risks in the cloud and guide security efforts. As described in Sec. III, in addition to the published IP ranges of these major providers, we also included IP ranges with usage type *DCH* and *CDN* from IP2Location [5] to represent other cloud providers. In Table III, we present the share of these major providers compared to the remaining cloud providers, which we refer to as *other*. This category includes IPs that IP2location considers as clouds based on their usage type, but they are not in the published IP ranges of major cloud providers. Upon an additional investigation, we found out that a large part of those IPs belong to the cloud providers themselves for Software as a Service (SaaS) infrastructure (*e.g.,* Google hosting Gmail for workspace, where customers can use their domain for emails).

Table III shows a longitudinal analysis from 2021–2025, revealing how the share of blocked domains hosted by major providers has changed over time. We elaborate on this trend in Sec. IV-D2. In 2025, most of the domains are hosted by *other* cloud providers across all infrastructure categories.

For web hosting infrastructure (A), AWS has a comparable share to *other* (around 35%), indicating its significant contribution in web hosting. There is a visible difference between the percentage of blocked domains hosted by *other* providers (88.89%) and the baseline domains (61.87%), which shows web infrastructure for blocked domains is mostly spread among different cloud providers. The rest of the major providers have a higher share in baseline domains than in blocked domains, except for Azure and DigitalOcean, which show a higher share in blocked domains; this difference is more pronounced for Azure.

For DNS (NS), similar to A, other cloud providers dominate with over 90% in both baseline and blocked domains, and AWS leads among the five major providers. Other providers, Google, AWS, and DigitalOcean, have a higher percentage of blocked domains than the baseline, which is more noticeable in AWS.

For email (MX), consistent with the NS data, AWS, Google, and DigitalOcean are also more prominent in malicious infrastructure.

These observations suggest that while a few major cloud providers dominate each infrastructure component, most malicious infrastructure is spread across many others, reflecting attackers' diverse and decentralized choices. A possible reason is that major providers detect and respond to abuse more quickly, though our data does not confirm this directly.

### D. Longitudinal Analysis

To track the migration of malicious infrastructure to cloud providers, we compare cloud adoption in baseline and blocked domains at two points in time. Since the earliest consistent data across all datasets is from January 2021, we use that as the starting point. As noted in Sec. IV-C, our cloud dataset includes IP ranges from major providers (AWS, Google, Azure, Oracle) and IPs marked as *DCH* or *CDN* in IP2location, excluding DigitalOcean due to missing historical data. The 2025 baseline and blocklisted datasets contain 178,330,232 and 717,106 domains, respectively, compared to 142,448,498 and 323,610 in 2021.

*1) Cloud migration dynamics:* As described in Sec.IV-B, we created UpSet plots of domain infrastructure across cloud providers. Comparing the 2021 and 2025 distributions Fig.2, overall cloud use for individual DNS components (A, NS, MX) in the baseline remained stable, with fewer domains lacking cloud infrastructure. In 2021, about 44.1% of domains were using all three services in the cloud, but by 2025, that number dropped to 43.3%, indicating a small drop in full cloud migration. At the same time, the percentage of domains using just cloud-based web hosting and DNS without setting up email in the cloud grew. This partial setup rose from 36.7% to 39.7%, suggesting a shift toward selective rather than full adoption of cloud services.

This trend is even clearer when we look at blocked domains. Across the board, cloud usage in this group dropped, but there is a sharp increase in domains that use only cloud hosting, rising from 6.6% in 2021 to 26.4% in 2025. There's also a smaller increase in those using only cloud-based name servers. Meanwhile, the number of blocked domains using a fully cloud-based setup dropped significantly, from 35.1% to just 16%. Blocked domains show a similar trend to baseline domains, but with a stronger shift toward partial cloud use—especially for hosting—and a decline in full adoption. This suggests malicious actors increasingly favor hybrid setups, using cloud services selectively while keeping other

TABLE III: Cloud provider usage across A, NS, and MX infrastructures (baseline vs blocked domains 2021-2025)

| | 2021 | | | | | |
|---|---|---|---|---|---|---|
| | Other | | AWS | | Azure | |
| **Infra** | Baseline | Blocked | Baseline | Blocked | Baseline | Blocked |
| **A** | 91.2M (71.66%) | 230.4K (89.48%) | 11.2M (8.79%) | 12.9K (5.02%) | 463.7K (0.36%) | 1.1K (0.43%) |
| **NS** | 120.1M (94.41%) | 265.17K (95.60%) | 7.1M (5.56%) | 11.4K (4.13%) | 237.3K (0.19%) | 403 (0.15%) |
| **MX** | 65.4M (96.63%) | 114.9K (94.04%) | 2.2M (3.22%) | 7.0K (5.71%) | 56.1K (0.08%) | 273 (0.22%) |
| | 2025 | | | | | |
| **A** | 79.8M (61.87%) | 500.3K (88.89%) | 44.9M (34.82%) | 37.7K (6.69%) | 589K (0.45%) | 20.3K (3.60%) |
| **NS** | 125.1M (94.88%) | 463.9K (95.84%) | 8.1M (6.16%) | 50.5K (10.43%) | 470.5K (0.36%) | 969 (0.20%) |
| **MX** | 57.2M (84.93%) | 109.5K (78.32%) | 1.6M (2.39%) | 4.3K (3.09%) | 6.6M (9.83%) | 3.0K (2.14%) |

| | 2021 | | | | | |
|---|---|---|---|---|---|---|
| | Google | | DigitalOcean | | Oracle | |
| **Infra** | Baseline | Blocked | Baseline | Blocked | Baseline | Blocked |
| **A** | 24.6M (19.34%) | 13.1K (5.10%) | - | - | 57.3K (0.05%) | 47 (0.02%) |
| **NS** | 1.2M (0.97%) | 2.0K (0.74%) | - | - | 3.0K (0.002%) | 8 (0.002%) |
| **MX** | 856K (1.26%) | 1.3K (1.05%) | - | - | 2.8K (0.004%) | 11 (0.009%) |
| | 2025 | | | | | |
| **Infra** | Baseline | Blocked | Baseline | Blocked | Baseline | Blocked |
| **A** | 2.77M (2.15%) | 12.0K (2.13%) | 1.04M (0.81%) | 5.4K (0.96%) | 89.9K (0.07%) | 108 (0.02%) |
| **NS** | 1.06M (0.80%) | 8.2K (1.70%) | 847.7K (0.64%) | 10.6K (2.19%) | 10.0K (0.007%) | 8 (0.001%) |
| **MX** | 1.4M (2.12%) | 6.9K (4.94%) | 1.6M (2.34%) | 21.5K (15.38%) | 44.2K (0.07%) | 17 (0.01%) |

components outside the cloud to evade detection, boost resilience, or limit dependence on a single provider.

*2) Cloud provider adoption dynamics:* Comparing the values in Table III, a consistent pattern emerges across 2021 and 2025: Azure's presence increases across all three infrastructure types, while providers in the *other* category continue to dominate across all categories and Oracle remains the least-used provider throughout. For web hosting (A), the share of baseline domains hosted by other cloud providers dropped significantly from 71.66% to 61.87%, while the drop for blocked domains was minimal. This makes the gap between blocked and baseline domains more notable in 2025 and highlights that malicious actors still prefer to rely on a wider variety of cloud providers. AWS's share of web hosting for baseline domains rose sharply from 8.79% in 2021 to 34.82% in 2025, while its role in hosting blocked domains remained limited, suggesting stronger security measures in its web hosting infrastructure. Azure showed the opposite trend: despite only a slight increase in the baseline, its share of blocked domains grew from 0.43% to 3.60%. Google's share declined in both baseline and blocked domains, with a significant decrease in the baseline.

In the NS category, AWS shows a reverse approach than in A, with a slight increase in the baseline, the percentage of blocked domains grows more from 4.13% to 10.43%. The share of blocked domains using Google-hosted name servers also increased in this period.

For email (MX), the share of domains using mail servers in the *other* category dropped significantly, especially among blocked domains. This aligns with our findings in Sec. IV-D1 and suggests that domain owners—particularly malicious actors—tend to avoid hosting their full infrastructure stack in the cloud. Meanwhile, the percentage of domains using Google-, Azure-, and Oracle-hosted mail servers increased from 2021 to 2025.

These findings indicate that adversaries still prefer to use a wider range of cloud providers and are reluctant to host all parts of their infrastructure in the cloud, especially mail services.

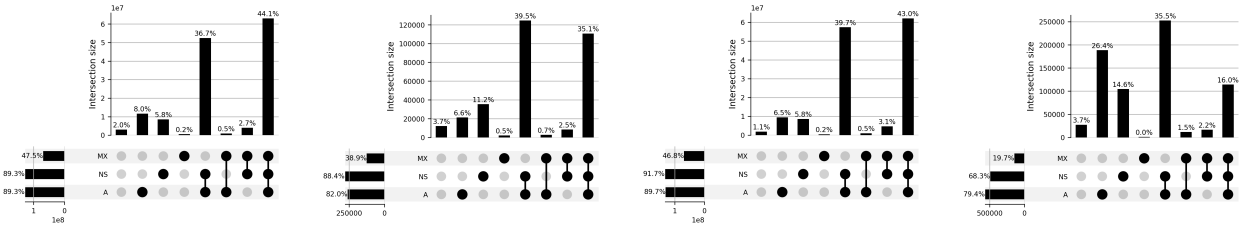
## V. LIMITATIONS

As with any empirical study, our results have limitations. We relied on IP2Location, a commercial dataset with opaque classification that may misclassify cloud resources. Some domains had incomplete infrastructural data, limiting full analysis. Historical data were unavailable for certain providers (e.g., DigitalOcean), constraining longitudinal results. Finally, our blocklist covers only part of malicious activity, missing some types of abuse (*e.g.,* transient [25] and compromised [23] domains) and we focused only on *.com* domains, so our findings may under-represent certain forms of malicious infrastructure.

## VI. DISCUSSION AND CONCLUSION

Our analysis shows that malicious domains increasingly adopt partial cloud migration, primarily outsourcing web hosting and DNS while avoiding full cloud reliance. This trend was mild in general domains but more evident in blocklisted ones, highlighting attackers' preference for hybrid setups that balance cost, resilience, and evasion. From an operational standpoint, this implies that providers should extend monitoring beyond fully hosted infrastructures and develop methods to detect fragmented or mixed deployments.

At the provider level, AWS dominates hosting for general domains, while GoDaddy leads DNS, yet neither contributes significantly to malicious infrastructure. Instead, abuse is more dispersed across other providers, suggesting that market share does not directly translate to abuse prevalence. The factors such as security policies,




(a) Baseline (Jan 2021) (b) Blocked (Jan 2021) (c) Baseline (Jan 2025) (d) Blocked (Jan 2025)

Fig. 2: UpSet plots of domains infrastructural distribution in clouds (2021 vs 2025).

costs, and responsiveness likely shape these differences. Distributional patterns across infrastructure components show a general alignment between a country's overall hosting rate and its share of malicious infrastructure; countries with more domains are generally highly likely to host more malicious ones. However, this correlation is not strong for ASNs, which may be due to factors such as niche providers. Importantly, a strong country-level correlation does not imply a higher prevalence of malicious domains; some countries with relatively few domains still host many malicious ones. Similar variability appears across ASNs, where providers of similar size show different maliciousness ratios.

These findings underscore the operational complexity of detecting cloud abuse. Mitigation requires better collaboration between providers, shared abuse intelligence, clearer cloud classifications, and stronger detection of hybrid setups with coordinated takedowns.

Future work should extend beyond the *.com* namespace, incorporate broader blocklists and providers, and investigate attackers' outsourcing motivations alongside provider countermeasures. Overall, our results highlight the need for dynamic, cooperative, and transparent approaches to secure the evolving cloud ecosystem.

## Acknowledgments

This work was funded by the Centrum voor Veiligheid en Digitalisering (CVD) and NWO under grant NWA.1215.18.003 (CATRIN), and was partially supported by the GÉANT GN5-2 programme, funded by the European Commission.

## References

[1] AWS IPs. https://ip-ranges.amazonaws.com/ip-ranges.json.
[2] Azure IPs. https://www.microsoft.com/en-us/download/details.aspx?id=56519.
[3] DigitalOcean IPs. https://digitalocean.com/geo/google.csv.
[4] Google IPs. https://www.gstatic.com/ipranges/cloud.json.
[5] IP2Location. https://www.ip2location.com/.
[6] AWS: Zeus Botnet Controller. https://aws.amazon.com/security/security-bulletins/zeus-botnet-controller/, 2009.
[7] Cybercrime-tracker. https://cybercrime-tracker.net/, 2024.
[8] DigitalSide Repository. https://osint.digitalside.it/, 2024.
[9] Domain Blocklist (DBL). https://www.spamhaus.org/blocklists/domain-blocklist/, 2024.
[10] OpenPhish. https://openphish.com/, 2024.
[11] Oracle DynDNS Malware Feeds. http://security-research.dyndns.org/pub/malware-feeds/, 2024.
[12] Oracle IPs. https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json, 2024.
[13] PhishingArmy. https://phishing.army/, 2024.
[14] PhishTank. https://phishtank.org/, 2024.
[15] QuidsUp. https://quidsup.net/notrack/blocklist.php, 2024.
[16] Tolouse Blacklists. https://dsi.ut-capitole.fr/blacklists/, 2024.
[17] VxVault. http://vxvault.net/ViriList.php, 2024.
[18] Domain Name Statistics by TLD Type. https://domainnamestat.com/statistics/tldtype/all, 2025.
[19] M. Allegretta, G. Siracusano, R. González, M. Gramaglia, and J. Caballero. Web of shadows: Investigating malware abuse of internet services. *Comput. Security*, 149:104182, 2025.
[20] S. Alrwais, X. Liao, X. Mi, P. Wang, X. Wang, F. Qian, R. Beyah, and D. McCoy. Under the shadow of sunshine: Detecting bulletproof hosting on legitimate service provider networks. In *Proc. IEEE S&P*, pages 805–823, 2017.
[21] G. Kontaxis, I. Polakis, and S. Ioannidis. Outsourcing malicious infrastructure to the cloud. In *Proc. IEEE SysSec*, 2011.
[22] X. Liao, S. Alrwais, K. Yuan, L. Xing, X. Wang, S. Hao, and R. Beyah. Lurking malice in the cloud: Detecting cloud repository as a malicious service. In *Proc. ACM CCS*, pages 1541–1552, 2016.
[23] S. Maroofi, M. Korczyński, C. Hesselman, B. Ampeau, and A. Duda. Comar: Classification of compromised versus maliciously registered domains. In *Proc. IEEE EuroS&P*, pages 607–623, 2020.
[24] NSI. The State of Cloud Ransomware in 2024. https://www.nsi-ca.com/blog/the-state-of-cloud-ransomware-in-2024, 2024.
[25] R. Sommese, G. Akiwate, A. Affinito, M. Müller, M. Jonker, and K. C. Claffy. Darkdns: Revisiting the value of rapid zone update. In *Proc. ACM IMC*, pages 454–461, 2024.
[26] R. Sommese, G. C. M. Moura, M. Jonker, R. van Rijswijk-Deij, A. Dainotti, K. C. Claffy, and A. Sperotto. When parents and children disagree: Diving into dns delegation inconsistency. In *Proc. PAM*, 2020.
[27] R. Tandon, J. Mirkovic, and P. Charnsethikul. Quantifying cloud misbehavior. In *Proc. IEEE CloudNet*, pages 1–8, 2020.
[28] S. Tarahomi, R. Holz, and A. Sperotto. Quantifying security risks in cloud infrastructures: A data-driven approach. In *Proc. IEEE NetSoft*, pages 346–349, 2023.
[29] S. Tarahomi, R. Sommese, P.-T. de Boer, J. Linssen, R. Holz, and A. Sperotto. Is a name enough? detecting clouds using dns pointer records. In *Proc. IEEE CNSM*, pages 1–5, 2024.
[30] R. van Rijswijk-Deij, M. Jonker, A. Sperotto, and A. Pras. A high-performance, scalable infrastructure for large-scale active dns measurements. *IEEE J. Sel. Areas Commun.*, 2016.
[31] R. Yazdani, M. Resing, and A. Sperotto. Glossy mirrors: On the role of open resolvers in reflection and amplification ddos attacks. In *Proc. IEEE CNSM*, pages 1–9, 2024.
[32] B. Z. H. Zhao, M. Ikram, H. J. Asghar, M. A. Kaafar, A. Chaabane, and K. Thilakarathna. A decade of mal-activity reporting: Retrospective analysis of blacklists. In *Proc. ACM Asia CCS*, pages 193–205, 2019.
[33] J. Zirngibl, S. Deutch, P. Sattler, J. Aulbach, G. Carle, and M. Jonker. Domain parking: Largely present, rarely considered! In *Proc. TMA*, 2022.