Measuring the Adoption of DDoS Protection Services

Mattijs Jonker
University of Twente
m.jonker@utwente.nl

Anna Sperotto
University of Twente

Roland van Rijswijk-Deij
University of Twente and SURFnet bv

Ramin Sadre
Université catholique de Louvain

Aiko Pras
University of Twente

ABSTRACT

Distributed Denial-of-Service (DDoS) attacks have steadily gained in popularity over the last decade, their intensity ranging from mere nuisance to severe. The increased number of attacks, combined with the loss of revenue for the targets, has given rise to a market for DDoS Protection Service (DPS) providers, to whom victims can outsource the cleansing of their traffic by using traffic diversion.

In this paper, we investigate the adoption of cloud-based DPSs worldwide. We focus on nine leading providers. Our outlook on adoption is made on the basis of active DNS measurements. We introduce a methodology that allows us, for a given domain name, to determine if traffic diversion to a DPS is in effect. It also allows us to distinguish various methods of traffic diversion and protection. For our analysis we use a long-term, large-scale data set that covers well over 50% of all names in the global domain namespace, in daily snapshots, over a period of 1.5 years.

Our results show that DPS adoption has grown by 1.24× during our measurement period, a prominent trend compared to the overall expansion of the namespace. Our study also reveals that adoption is often lead by big players such as large Web hosters, which activate or deactivate DDoS protection for millions of domain names at once.

Keywords

DDoS attack mitigation; cloud-based security; protection networks; protection services; active DNS measurements

1. INTRODUCTION

In recent years, we have seen a rise of a simple yet very effective class of attacks: (Distributed) Denial of Service attacks (DDoS) [1]. These can easily generate traffic volumes in the order of hundreds of Gbps. Recent attacks reached 300-600Gbps (e.g., on Spamhaus in 2013 [2], or on BBC in 2016 [3]). To make things worse, on-demand attacks can easily be purchased online for only a few USD [4, 5], which has further increased the popularity of such attacks.

The growth in number of attacks [6], combined with the loss of revenue for the targets, has given rise to a market for DDoS Protection Service (DPS) providers. The protection of a specific application, or even an entire network, can be outsourced to a DPS. Protection can take place on-site, by means of dedicated appliances [7], or be handled in the cloud, where malicious traffic is filtered or absorbed, thus effectively thwarting the attack. Hybrid solutions also exist, where on-site appliances are combined with a cloud-based component. Attacks can be volumetric (i.e., saturating the target's bandwidth) or semantic (e.g., denying service access with minimal bandwidth effects).

Traffic diversion is the key mechanism that allows traffic to be routed through the DPS infrastructure, either in an always-on or on-demand manner. An effective way to divert traffic for applications that are reached on the basis of a domain name, is to exploit the Domain Name System (DNS), similarly to what is done in content delivery networks for implementing load balancing [8, 9]. An alternative is to use the Border Gateway Protocol (BGP) to divert traffic towards the DPS infrastructure.

In this paper, we investigate the adoption of cloud-based DPSs worldwide. We focus on nine leading providers according to [13], namely Akamai, CenturyLink, CloudFlare, DOSarrest, F5 Networks, Incapsula, Level 3, Neustar, and Verisign. Our investigation is done on the basis of long-term, active DNS measurements, which allows us, for a given domain name, to verify if traffic diversion towards a DPS is in place. Our large-scale data set consists of daily measurements, over a period of 1.5 years, of the entire `.com`, `.net` and `.org` zones, which contain about 50% of names in the global domain namespace [10]. It also contains half a year's worth of measurements for the `.nl` zone, as well as for domain names on the Alexa Top 1M list[1].

Our study not only confirms an increasing adoption of DPSs, but it also shows a growth of 1.24× in the zones we studied for 1.5 years, against an overall growth of these zones of only 1.09×. In addition, when looking at the breakdown of the data set per DPS, our results show the emergence of big players, such as large Web hosters and domainers, which indicates that the adoption trends are not led by single users but by larger parties.

We explain the various traffic diversion approaches in Section 2. Our measurement and analysis methodology is described in Section 3, completed by an overview on the studied data set. We present and discuss our findings and results in Section 4, and conclude in Section 5.

IMC 2016, November 14-16, 2016, Santa Monica, CA, USA
© 2016 ACM. ISBN 978-1-4503-4526-2/16/11...$15.00
DOI: http://dx.doi.org/10.1145/2987443.2987487

[1] http://www.alexa.com/

2. DDOS PROTECTION SERVICES

DPS providers can offer cloud-based, in-line, or hybrid solutions. The type of attack (i.e., volumetric or semantic) and customer determine the potential of each solution. For example, an ISP may require BGP-based protection of a network, but the owner of a popular Web site needs only to divert traffic destined to single host. As another example, banks want to terminate encrypted e-banking connections themselves, and therefore require a hybrid solution in which the in-line appliance mitigates semantic attacks, while the cloud thwarts large volumetric attacks. For all but strictly in-line solutions, traffic diversion is required.

In the remainder of this section we outline the functioning of widely used diversion mechanisms based on DNS and BGP, and how those are implemented in a DPS.

2.1 DNS-based Network Traffic Diversion

DNS can be used in various ways to divert network traffic, as long as the asset to be protected is reached through a domain name:

Address record – The owner of a domain name can (directly) set an `A` record to a DPS-assigned IP address.[2] An example is shown below. The name server `ns.registr.ar` is authoritative for the DNS zone of the domain `www.examp.le`, as is indicated by the `NS` record.

```
;; ANSWER SECTION:
www.examp.le   IN  A   10.0.0.1
;; AUTHORITY SECTION:
www.examp.le   IN  NS  ns.registr.ar
```

Canonical Name – A domain name can be made into an alias for another with the `CNAME` record. If the `CNAME` record of x references the canonical name y, then through so-called name expansion some record types for x are determined by the DNS zone of y. This means the DNS zone of y can, among others, set x's IP addresses. In the example shown below, the domain `foob.ar` belongs to the DPS, which through its authoritative name server allows the DPS to affect the IP addresses for `www.examp.le`.

```
;; ANSWER SECTION:
www.examp.le   IN  CNAME   foob.ar
foob.ar        IN  A       10.0.0.2
;; AUTHORITY SECTION:
foob.ar        IN  NS      ns.foob.ar
```

Name Server – The DNS zone of a domain can be delegated to a name server which belongs to a DPS. Unlike the `CNAME` use case, the DPS provider is now able to change the address records of the protected domain. An example is shown below, in which the name server of the DPS, `ns.foob.ar`, is authoritative for `www.examp.le`.

```
;; ANSWER SECTION:
www.examp.le   IN  A   10.0.0.2
;; AUTHORITY SECTION:
www.examp.le   IN  NS  ns.foob.ar
```

The difference between the outlined `CNAME` and `NS` cases is one that relates to full control over DNS records. In the `CNAME` example above, the DPS-controlled `ns.foob.ar` is not authoritative for `www.examp.le`. In effect, the DPS cannot change any of `www.examp.le`'s records, even though it can affect IP address records through the `CNAME`'s expansion.

It is commonplace for DPS providers to combine a DNS-based diversion approach with a reverse proxy for, e.g., requests to protected Web sites. In such a setup, Web content is pulled from the customer by forwarding the request. Next, the request is answered from within the DPS infrastructure. The customer should drop the requests that are not made by the DPS because DNS can be bypassed to launch direct attacks [11].

2.2 BGP Prefix Announcements

BGP can be used to divert network traffic to a DPS. This requires the DPS to announce an IP subnet of its customer, such as a */24*. All traffic destined for the customer's subnet is then routed to the DPS infrastructure for scrubbing. After scrubbing, traffic is sent back to the customer's network by means of, e.g., a Generic Routing Encapsulation (GRE) tunnel. A BGP-based approach is typically used to protect entire networks or when a reverse proxy is not feasible.

2.3 Moment of Mitigation

Diversion can be done in an *on-demand* or *always-on* manner. In the case of *always-on* DDoS protection, traffic is *always* routed to the DPS infrastructure, even if a customer is not under attack. Thus, if DNS-based diversion is used, an address lookup always results in an IP address that routes to the DPS infrastructure. In the BGP case the DPS will never withdraw the customer's IP subnet announcement.

If protection is done *on-demand*, a DNS change is made by either the provider or the customer, or the DPS could start announcing a customer's IP prefix using BGP. For the prior, the DNS change depends on the method of use:

- **Address record** – The owner of a domain changes its address records from an IP address that does not route to the DPS infrastructure to a DPS-assigned IP address. Multiple address records may need to be changed if the domain has more than one. All changes can later be reverted to stop diverting traffic.
- **Canonical Name** – Since the DPS controls the authoritative name server for the canonical domain name, changes can be made in a manner similar to that outlined above.
- **Name Server** – The DPS controls the authoritative name server for the protected domain name and as such it can change the address record(s) accordingly.

On-demand protection can be manual or automated. As an example of the latter consider customer-premise mitigation equipment (i.e., an in-line appliance) that sends out an alert to the DPS in case an attack is too large to handle in-line. In such a hybrid approach, the DPS can initiate *on-demand* protection automatically.

3. METHODOLOGY AND DATA SET

To study the use of DDoS protection services we use data from active DNS measurements over a period of 1.5 years, for a large set of domain names. We analyze the measurement data using Hadoop to identify whether and how domains are protected by a DPS. The various steps of the measurement and analysis process, as well as general statistics of the resulting data set, are described next.

[2] Depending on how the DPS operates, the IP address can either be customer-specific, or shared among customers in a "cloud-based" manner. Moreover, in case IPv6 is supported, the `AAAA` RR can be set accordingly.

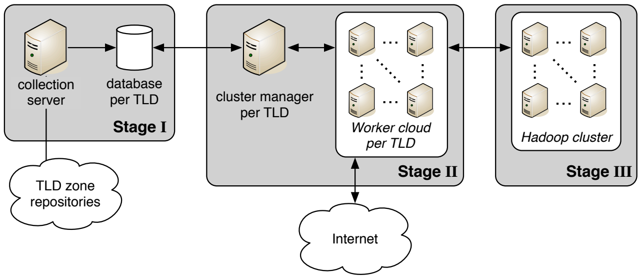

Figure 1: Architecture of our measurement system

3.1 Active DNS Measurements

In earlier work, we designed and implemented a measurement system for large-scale, active DNS measurements [12]. This system queries a chosen set of RRs for a given list of domains, and it repeats these measurements daily. Among others, it queries for `A`, `AAAA`, and `NS` records. `A` and `AAAA` queries are sent not only for the root label (i.e., apex) of a domain, but also for other common labels, such as `www`. This means for a given domain `name`, both `name.com` and `www.name.com` are queried. All fields from the answer section of a DNS response are stored, which includes `CNAMEs` and their full expansions.

A high-level view of our system is shown in Figure 1. The measurement starting point is a list of domain names. We primarily measure entire zones, i.e., the full list of names in a top-level domain (TLD), for which the system downloads updated zone files daily from registry operators. Secondarily we measure smaller lists, such as the Alexa Top 1M ranking. In this paper we focus mainly on measurement data for `.com`, `.net`, and `.org`, which together contain about 50% of the global domain namespace, which we have been measuring the longest. We also cover measurements for the country-code TLD `.nl`, and for domains on Alexa's Top 1M list.

3.2 Supplementing AS Numbers

We supplement each IP address with an autonomous system number (ASN) on the basis of BGP data. The origin AS of the most-specific prefix in which an address was contained at measurement time is determined on the basis of the Routeviews Prefix-to-AS mappings (pfx2as) data set[3].[4]

3.3 Deriving DDoS Protection Service Use

We analyzed the measurement data to detect the use of DPS providers. Several of the studied providers offer DNS-based traffic diversion and (optionally) authoritative name server protection.

As detailed in Section 2, various ways exist to divert network traffic to the infrastructure of a DPS. Our analysis reveals, per day, if domain x uses one (or several) of these methods. More specifically, we detect `CNAME`-based redirection by checking whether the `CNAME` expansion of x contains a DPS reference. Similarly, the `NS` record of x will reference a DPS if the DNS zone of x is managed by that DPS. Lastly, the ASN of x's IP address(es) can also reference a DPS.

We detect DPS references in `CNAME` and `NS` records based on the second-level domain (SLD) contained therein. For example, we found that Incapsula uses the SLD *incapdns.net* in `CNAME` records. To identify SLD and ASN references, we apply the following procedure. We take the ASNs of a DPS as starting point.[5] Then we find all the domain names that reference these ASNs and analyze frequently occurring SLDs in `CNAME` and `NS` records. The SLDs obtained in this manner are used to find any ASNs we may have missed in the first step, or to remove ASNs that do not belong to the mitigation infrastructure of a DPS.

Source	start	days	#SLDs	#DPs	size
`.com`	2015-03	550	161.2M	534.5G	17.5TiB
`.net`	2015-03	550	20.2M	62.4G	2.1TiB
`.org`	2015-03	550	13.8M	46.7G	1.5TiB
`.nl`	2016-03	184	5.9M	10.4G	2.1TiB
Alexa 1M	2016-03	184	2.2M	1.7G	77.5GiB
Total			203.3M	655.7G	23.3TiB

Table 1: Data set

Based on combinations of references and non-references we can analyze not only if, but also how a domain uses a DPS. Take for example a domain that references a DPS by `CNAME` and ASN, but not by `NS` record. This combination of references shows us not only that the domain uses `CNAME`-based redirection to effectively divert traffic to a DPS. Moreover, we learn that the DNS zone of this domain has not been delegated to the DPS.

By evaluating combinations of references we also identify frequently-used third parties, such as third-party name servers that are authoritative for large numbers of domains that switch on or off protection simultaneously.

3.4 Always-on and On-demand Use

To analyze if a domain uses a DPS in an *always-on* or *on-demand* manner, we track (non-)use of the DPS by the domain over the measurement duration. If a domain always references a DPS by ASN, i.e., without gap days, we assume *always-on* use. *On-demand* use is assumed if a domain switches back and forth between two IP addresses over time of which the prior does not and the latter does reference a DPS. In this case, `CNAME`, `NS`, and ASN (non-)references reveal specifically how *on-demand* traffic diversion was effected. For example, a domain for which the ASN of an unchanged IP address references a DPS on and off suggests BGP-based traffic diversion.

3.5 Data Set

Our data set contains 1.5 years worth of measurements for the generic TLDs (gTLDs) `.com`, `.net`, and `.org`, in addition to six months for the country-code TLD (ccTLD) `.nl` and for the Alexa Top 1M. Table 1 details the data set. The column *#SLDs* shows the number of unique SLDs observed over the measurement period. *#DPs* is the number of collected data points (i.e., `CNAME`, `A`, `AAAA`, and `NS` measurements[6]). The *size* column shows the compressed measurement data size in our cluster using Parquet columnar storage[7] (before replication). The three gTLDs contain about 50% of the global domain namespace; on the last day of the data set they contain a little over 152M names.

Table 2 shows the ASN and SLD references for the considered DPS providers, obtained using the procedure described

[3] www.caida.org/data/routing/routeviews-prefix2as.xml

[4] For multi-origin AS we add all the involved AS numbers.

[5] We use AS-to-name data to find a DPS's AS numbers.

[6] AS numbers are supplement and not counted separately.

[7] https://parquet.io/

Provider	AS number(s)	CNAME second-level domain(s)	NS second-level domain(s)
Akamai	20940, 16625, 32787	*akamaiedge.net, edgekey.net, edgesuite.net, akamai.net*	*akam.net, akamai.net, akamaiedge.net*
CenturyLink	209, 3561	—	*savvis.net, savvisdirect.net, qwest.net, centurytel.net, centurylink.net*
CloudFlare	13335	*cloudflare.net*	*cloudflare.com*
DOSarrest	19324	—	—
F5 Networks	55002	—	—
Incapsula	19551	*incapdns.net*	*incapsecuredns.net*
Level 3	3549, 3356, 11213, 10753	—	*l3.net, level3.net*
Neustar	7786, 12008, 19905	*ultradns.net*	*ultradns.* (e.g., .com & .biz)*
Verisign	26415, 30060	—	*verisigndns.com*

Table 2: DDoS Protection Service provider references

in Section 3.3.[8] Some providers do not work with `CNAME` redirection, but through delegation can *change* the IP address of a domain (e.g., Verisign's *Managed DNS service*). Some providers (e.g., F5 Networks & DOSarrest) offer none of the DNS options.

4. RESULTS

4.1 General Overview

Using the references in Table 2, we analyze the three main TLDs and find per day the number of domains that use the DPS providers under consideration.[9] Fig. 2 shows the variation of the number of distinct SLDs over time. The figure is dominated by many "anomalous" peaks and troughs, which can involve millions of domains. For example, the peak on the 5th of March, 2015 involves about *1.1M* domain names. The anomalous trend that is apparent in the largest gTLD, `.com`, is replicated in `.net` and `.org`, which indicates that the anomalous behavior is transversal to the zones. Many of the larger anomalies are part of *on-demand* behavior, which we discuss in more detail in Section 4.4.

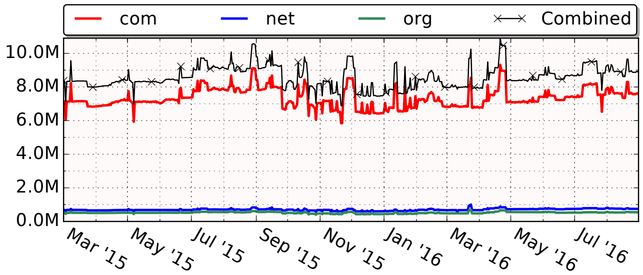

Figure 2: DPS use and zone breakdown

Fig. 3 shows over time per DPS the number of domains that use any of the DPS's services (the top line). As can be seen, some of the larger anomalies can be traced to Incapsula (e.g., the previously mentioned peak in March 2015 in Fig. 2). Some providers show very few anomalies, and contain more domains than the more anomalous providers on their "quiet" days. For example, CloudFlare versus Incapsula in March 2015, were it not for the anomalous peak.

In Fig. 4 we show the (average) distribution of the three main TLDs over the roughly 50% of the global domain namespace that they cover, as well as the distribution of DPS using domains among these TLDs. Both distributions are remarkably similar, suggesting that there is no correlation between a zone and subscribing to a DPS.

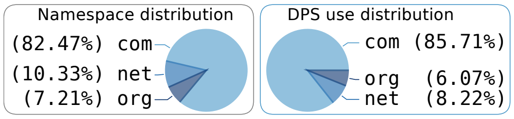

Figure 4: DPS use and gTLD distribution over namespace

4.2 Overall Growth

For our growth analysis we do not count anomalous peaks and troughs. We smooth shorter and smaller anomalies out by taking the median reference count over a time window of several weeks, while the large anomalies are cleaned manually. This way we largely separate *always-on* from *on-demand* use. Fig. 5 shows the combined growth of the nine providers relative to the start of our data set, in about 50% of the global domain namespace. The overall expansion of the zones involved is also shown. A trend in the adoption of DPSs becomes apparent, which is largely driven by CloudFlare, DOSarrest, Incapsula, and Verisign (cf. Fig. 3). Other providers such as F5 Networks and CenturyLink contribute to incidental decrease (e.g., the dip in March 2016). As shown, DPS use has grown by 1.24× over 1.5 years, which exceeds the overall expansion of 1.09×, from about *140M* to *152M* domains.

We applied the same procedure to our six-month data set for `.nl` and the Alexa Top 1M. Fig. 6 shows the results. A growth trend of *10.5%* against *1.8%* is shown for `.nl`, and for Alexa the growth is *11.8%*.

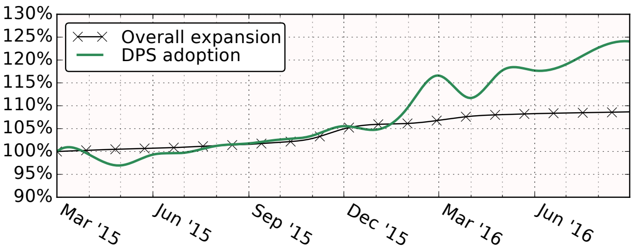

Figure 5: Growth of DPS use in 50% of the DNS

[8] It should be noted that for some of the studied providers the references can overlap with customers of other services. For example, for Akamai more than just *Kona Site Defender* (their reverse proxy) and *Prolexic Routed/Connect* (their BGP-based mitigation solution) domains can be traced to the found AS references.

[9] We consider use by domains on their second level, meaning that multiple references in the DNS zone of a domain are counted as one.

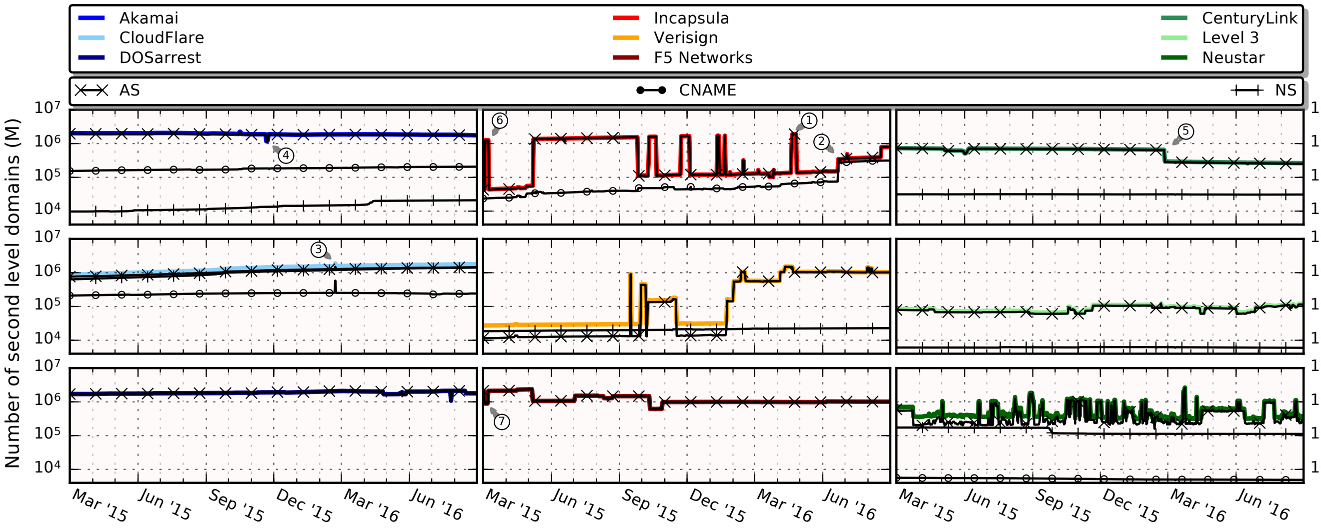

Figure 3: DPS use per provider and protection method breakdown

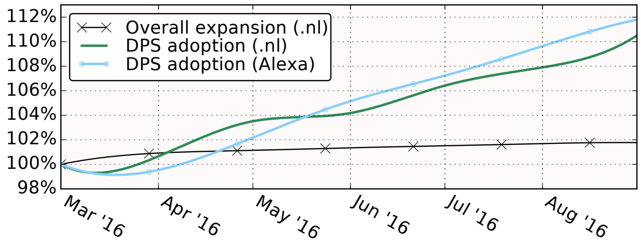

Figure 6: Growth of DPS use in `.nl` and Alexa

4.3 Protection Methods

As outlined in Section 2.1, various ways exist to use the DNS to divert network traffic to a DPS. Our reference analysis has shown that a DPS may support more than one way (cf. Table 2). Fig. 3 shows per DPS a breakdown of the various use cases (the marked `NS`, `CNAME`, and AS lines).

Difference in use among the nine DPS providers can be discerned, even where providers support the same DNS use cases. For example, if we look at the use of delegation, we find that CloudFlare's authoritative name servers are used significantly, by about *75%* of CloudFlare-using domains on average (compare CloudFlare's `NS` and overall, top line). For Incapsula, however, only about *0.02%* of domains use delegation, i.e., are using the *Incapsula NS Protection* service (this `NS` line is not visible). Verisign sits somewhere in the middle. During most of the first eleven months (March 2015 until February 2016), the number of Verisign-using domains that used delegation (i.e., their *Managed DNS* service) was even higher than those that diverted traffic (compare Verisign's `NS` and `AS` lines). We suspect that the dominant use of CloudFlare's *Authoritative DNS* among its customers, is because the service is free.[10]

4.4 Dynamic Behavior

4.4.1 Third-party Anomalies

We have traced many of the larger anomalies shown for each DPS to *on-demand* or *always-on* use by third parties, and in one case to a DNS issue at a third party. A few examples will follow. For **Incapsula**, Web site development platform *Wix* causes repeated swings of millions of domain names[11], such as the peak in April 2016 (cf. ①) that involves *1.76M* names. A second anomalous example for Incapsula is the increase in June 2016 (cf. ②), which we traced to "an opportunistic private equity fund around Internet domain names."[12] Most of **Verisign**'s larger anomalies can be traced to *ENOM* (a registrar) and *ZOHO*, accounting for changes of up to *700k* domains.[13] The February 2016 anomaly for **CloudFlare** (cf. ③) involves *∼247k Namecheap*-hosted domains.[14] The anomalous trough on November 22nd, 2015 for **Akamai** (cf. ⑥) was caused by *∼716k* domains that can be traced back to Sedo Domain Parking.[15] Our final example is the significant drop of domains in February 2016 for **CenturyLink** (cf. ⑤). We traced this to a platform that offers "Expert tools to manage domain registration, sales and monetization."[16] Some of the observed anomalies involve multiple providers. For example,

[10] We analyzed for a single day the set of full names of CloudFlare's authoritative name servers, most of which are given a male or female name, followed by *.ns.* and *cloudflare.com*, the `NS` SLD reference. There are 403 such names on April 30th, 2016, with *kate.ns.cloudflare.com* the most-referenced (by *112k* domains).

[11] Wix domains normally route to Amazon AWS (AS14618) through a *amazonaws.com* `CNAME`. During diversion, Wix name servers answer `A` records in various Wix-owned prefixes that are announced by Incapsula.

[12] This increase of about 170k domain names can be traced to SiteMatrix (a domainer).

[13] Several ENOM-owned */24s* route to Verisign (AS26415) during diversion, and to ENOM (AS21740) normally. Similar for ZOHO, with two prefixes normally in AS2639.

[14] The domains share a Namecheap `NS` SLD (i.e., *registrar-servers.com*) that answers CloudFlare-announced addresses.

[15] We infer that this was a DNS issue at Sedo, since the number of measured domains with a *sedoparking.com* `NS` SLD also dipped that same day.

[16] Here, a Fabulous-owned name server, starts giving `A` answers for *∼355k* domains that previously routed to two prefixes announced by CenturyLink's AS3561.

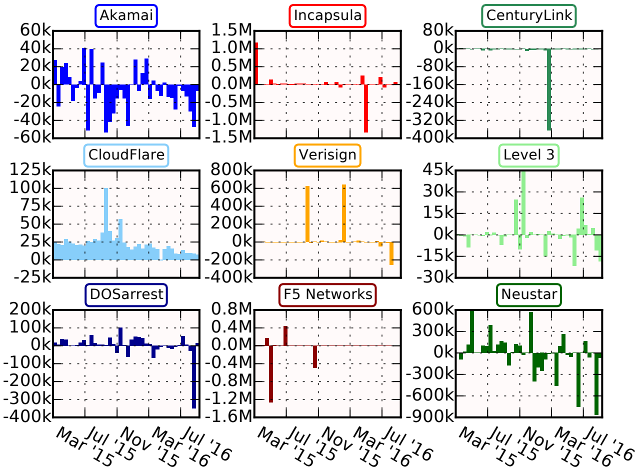

Figure 7: Flux of DPS use per provider

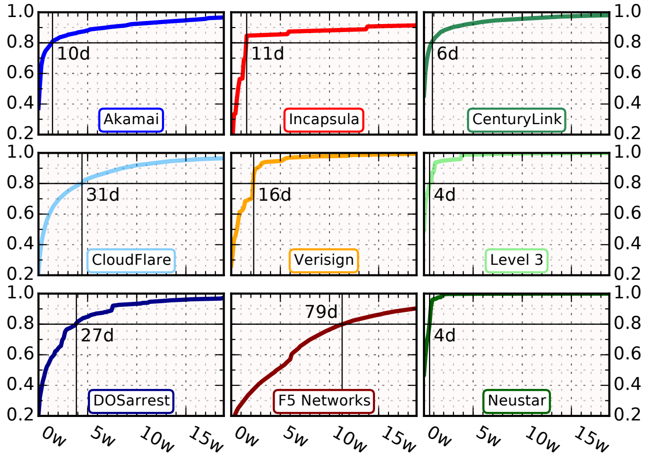

Figure 8: On-demand peak duration occurrences

the March 2015 peak for Incapsula has an opposing trough in F5 Networks (cf. ⑥ & ⑦).[17]

4.4.2 *Daily Fluctuations and Repeated Anomalies*

To study if repeated anomalies involve the same set of domain names, we analyzed the daily flux per provider in terms of first seen and last seen domain names. This way, if protection is turned on and off several times for a set of names, the names involved will contribute to influx at most once, and to outflux at most once. Fig. 7 shows per DPS the delta of first seen and last seen counts, in two-week time windows. As shown, repeated anomalies in Fig. 3 can be traced to the same sets of domain names[18]. For example, the large influx for Incapsula in March 2015 indicates that many of the same domains were involved in the anomalous plateau that starts in May 2015. A second take-away is that over time some providers contribute more gradually to DPS adoption than others, of which CloudFlare is a prime example, since its influx is rather spread out.

4.4.3 *On-demand Use*

Our outline of some of the larger anomalies shows that many can be traced to *on-demand* use, while some we suspect are *always-on* domains because of only an upward or downward edge. Since our measurement period is finite we cannot easily determine if an opposing edge can be found outside the measurement period. Moreover, a domain that shows a single period of use, i.e., peak, could either be a short-lived *always-on* customer, or brief *on-demand* use. Thus, it is not trivial to classify the type of DPS use. To gain more insight into dynamic behavior among the various providers we estimate for each a set of *on-demand* domains, which is done on the basis that the domains show at least three peaks over 1.5 years. For the sets of domain names, we analyzed the peak durations in days over the 1.5 year period. Fig. 8 shows the results as the CDF of peak occurrences. For providers that show signs of highly anomalous behavior from day to day, the majority of peak occurrences are short-lived (i.e., $P(duration <= days) = 0.8$). A good example is Neustar, with 80% of all peaks lasting four days or fewer, which we suspect is because their *always-on* solution is a hybrid[19] in which traffic is not continuously diverted to the cloud.

5. CONCLUSIONS

In this work we have shown that the adoption of DDoS Protection Services has grown significantly in the over 50% of the global domain namespace we studied. Our results show a relative growth of 1.24× over the previous 1.5 years, which surpasses the overall expansion of 1.09× of the considered namespace (i.e., `.com`, `.net`, and `.org`). Our results also show adoption trends in `.nl` and among domains on Alexa's Top 1M list, with growths of 1.11× and 1.12×, respectively, over a period of six months.

Our methodology can be used to analyze how domains divert traffic to a DPS, and whether or not optional services (e.g., name server protection) are used. In our results we reveal differences in use of protection methods among the considered providers, even in cases where the compared providers support similar services. For some providers, only a small percentage of domains use delegation, which potentially leaves a part of a domain's DNS infrastructure (i.e., the authoritative name server) susceptible to DDoS attacks.

Finally, our results show that a large contribution to the user base and adoption of DPS providers is made by third parties, examples of which are Web hosters and domainers. Some of these larger players activate or deactivate DDoS protection for millions of domains from one day to the next, either by leveraging the DNS to divert traffic, or by having the DPS announce one or multiple IP prefixes.

Acknowledgments

This work was supported by the EU-FP7 FLAMINGO Network of Excellence Project (318488). The research leading to these results was made possible by OpenINTEL[20], a joint project of the University of Twente, SURFnet, and SIDN. We thank our shepherd and the anonymous reviewers for their valuable feedback.

[17] Here, two Wix-owned prefixes switch back and forth from F5 Network's AS55002 to Incapsula's AS19551.

[18] Time grouping and variations in the customer base of third parties can change the flux magnitudes somewhat.

[19] https://www.neustar.biz/resources/faqs/ddos-faqs

[20] http://www.openintel.nl

6. REFERENCES

[1] Steve Mansfield-Devine. The evolution of DDoS. *Computer Fraud & Security*, 2014(10):15–20, 2014.

[2] Matthew Prince. The DDoS That Knocked Spamhaus Offline (And How We Mitigated It). https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/. Accessed: 2016-04-28.

[3] Swati Khandelwal. 602 Gbps! This May Have Been the Largest DDoS Attack in History. https://thehackernews.com/2016/01/biggest-ddos-attack.html. Accessed: 2016-05-12.

[4] Mohammad Karami and Damon McCoy. Understanding the Emerging Threat of DDoS-As-a-Service. Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET'13), 2013.

[5] José Jair Santanna, Roland van Rijswijk-Deij, Rick Hofstede, Anna Sperotto, Mark Wierbosch, Lisandro Zambenedetti Granville, and Aiko Pras. Booters – An Analysis of DDoS-as-a-Service Attacks. In *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM'2015)*, pages 243–251, 2015.

[6] Global DDoS Threat Landscape Q1 2016. https://www.incapsula.com/ddos-report/ddos-report-q1-2016.html. Accessed: 2016-04-28.

[7] John Pescatore. DDoS Attacks Advancing and Enduring: A SANS Survey. SANS, 2014.

[8] Cheng Huang, Angela Wang, Jin Li, and Keith W. Ross. Measuring and Evaluating Large-Scale CDNs. In *Microsoft Research Technical Report MSR-TR-2008-106*, October 2008. (full paper withdrawn from the 8th ACM SIGCOMM Conference on Internet Measurement (IMC'08)).

[9] Erik Nygren, Ramesh K. Sitaraman, and Jennifer Sun. The akamai network: A platform for high-performance internet applications. *SIGOPS Oper. Syst. Rev.*, 44(3):2–19, August 2010.

[10] The Domain Name Industry Brief. https://www.verisign.com/en_US/innovation/dnib/index.xhtml. Accessed: 2016-08-01.

[11] Thomas Vissers, Tom van Goethem, Wouter Joosen, and Nick Nikiforakis. Maneuvering Around Clouds: Bypassing Cloud-based Security Providers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 1530–1541, 2015.

[12] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE Journal on Selected Areas in Communications (JSAC)*, 34(6):1877–1888, 2016.

[13] Rick Holland and Ed Ferrara. The Forrester Wave^{TM}: DDoS Services Providers (Q3 2015). Forrester Research, Inc., July 2015.