Into the DDoS maelstrom: a longitudinal study of a scrubbing service

Giovane C. M. Moura[1], Cristian Hesselman[1,2],
Gerald Schaapman[3], Nick Boerman[4], Octavia de Weerdt[3]

WTMC 2020
2020-09-07

[1]SIDN Labs, [2]University of Twente, [3]NBIP, [4]SIDN

DDoS in the last years

- DDoS attacks aim at overwhelm a target, for multiple reasons
- They have become **cheaper, bigger** (record: 2.3Tb/s AWS), and more frequent
- You can buy DDoS-as-a-service nowadays, for a few Euros

'Nederlandse verdachte (18) eiste online zelf DDoS-aanvallen op'

De politie heeft een 18-jarige verdachte van DDoS-aanvallen gearresteerd. De jonge man werd opgepakt voor een DDoS-aanval waarmee de website van de Belastingdienst werd platgelegd. Eerder zou hij de Bunq bank hebben aangevallen. Volgens de bank gaat het om Jelle S. uit Oosterhout. Website Tweakers stelt dat de jongen zelf online de verantwoordelijkheid heeft opgeëist voor de aanvallen.

Chris Klomp 05-02-18, 16:59 Laatste update: 21:04

f 26

Figure 1: Teenager brings down banks, Dutch Tax Authority spending 40 EUR. Source: AD.nl
https://tinyurl.com/y5cofjs9/

Industry Response to DDoS

What can you do?

- Buy dedicated filtering hardware
- Use “cloud-based” services → re-route your traffic to be cleaned by someone else
  - typically metered (can become $$$)
  - can become very expensive
- NBIP created **NaWas**, a DDoS scrubbing service:
  - Buy hardware, share costs
  - **Not metered**
  - Members pay a flat-fee to cover OPs costs
  - Attack filtering activated on demand by members
  - 151 members (Jan. 2020) in NL and EU.

Industry Response to DDoS

What can you do?

- Buy dedicated filtering hardware
- Use “cloud-based” services $\rightarrow$ re-route your traffic to be cleaned by someone else
  - typically metered (can become $$$)
  - can become very expensive
- NBIP created **NaWas**, a DDoS scrubbing service:
  - Buy hardware, share costs
  - **Not metered**
  - Members pay a flat-fee to cover OPs costs
  - Attack filtering activated on demand by members
  - 151 members (Jan. 2020) in NL and EU.

We analyze NaWas datasets

- NaWas DDoS filtered datasets (22 months)

Attacks	1826
Targets (/32)	576
Prefixes Attacked	180
Autonomous Systems	65
Pool IPs (April 2019)	3,962,368

Table 1: DDoS attacks filtered at Nawas (July 2017 – May 2019)

	Duration (min)	*Peak (Gbps)*
25%ile	10	0.4
Median	20	1.4
Average	57	3.9
90%ile	98	13.1
Max	7560	79.0

Table 2: Duration and Peak Gpbs

Attacks Frequency and Size

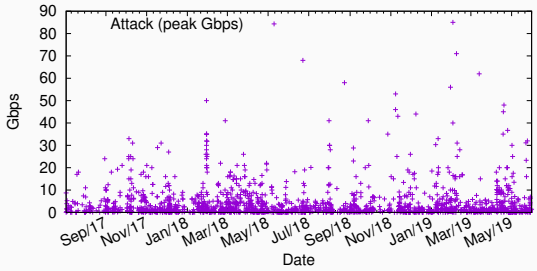

Figure 2: Attacks and Peak

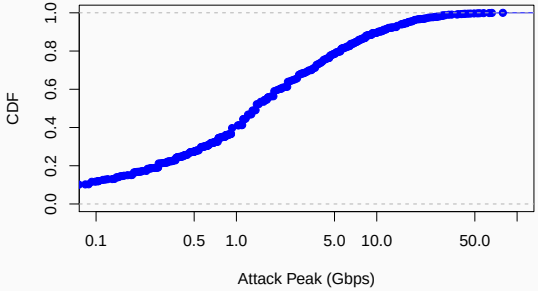

Figure 3: CDF of Attack Rates (peak)

Collateral Damage

- NaWas dataset only listed IPv4 addresses
- *What domains* were hosted on these IP addresses ?
- We look it up historically on OpenIntel

DNS Zone	Second-level domains	IPs
.nl	242,355	226
.com	72,180	178
.net	5,220	100
.org	5,314	94
Others	6,541	98
Total	331,610	576

Table 3: Collateral damage to Second-level domains on IPs under attack.

- 226 IPs hosted 242k domains (shared hosting)
- Collateral damage is much higher
- Victms are at least **the square** of the target IPs

Does DDoS leave its footprints on DNS?

- We saw 242 `.nl` domain names under attack
- We happen to run `.nl`
- is there evidence of DDoS on it?
- We look at daily queries for each domain
  - one week before
  - attack day

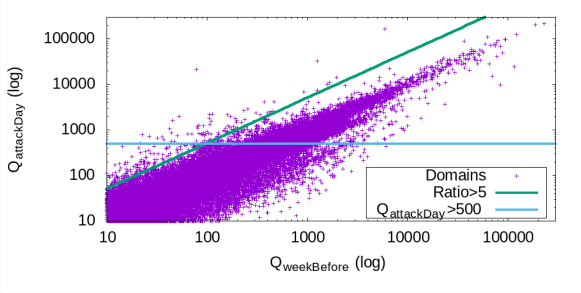

Figure 4: Domain names and number of queries on the attack day (*y* axis) and average daily week before it (*x* axis).

Dedicated hosting: 1IP$\rightarrow$ 1 domain

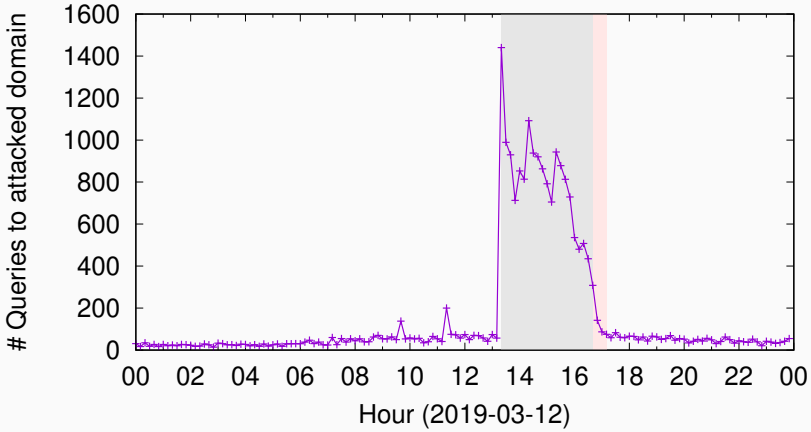

Figure 5: Pink area show area which scrubbing service was active; gray area shows when attacked started being noticed on DNS

Shared hosting: 1 IP $\rightarrow$ 6 domains

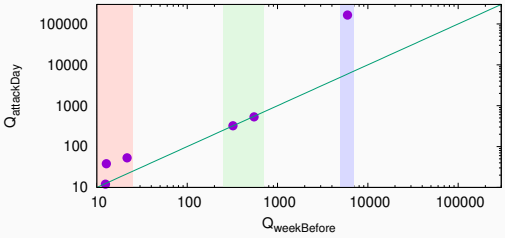

Figure 6: Shared hosting: 6 `.nl` domains, 1 targeted domain

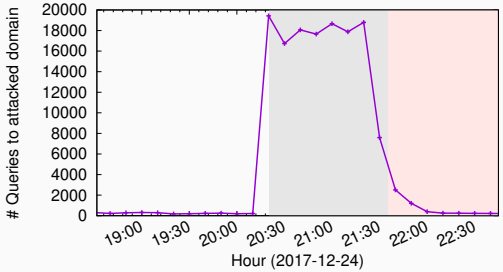

Figure 7: Timeseries of queries to targed domain from Fig. 6.

5 domains likely suffered alongside this targeted domain

Shared hosting: 1 IP $\rightarrow$ 6 domains

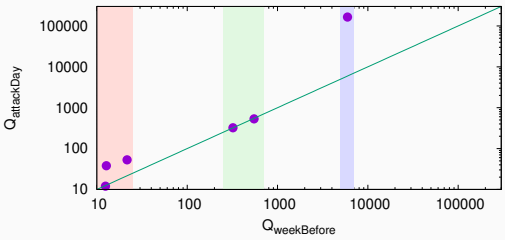

Figure 6: Shared hosting: 6 `.nl` domains, 1 targeted domain

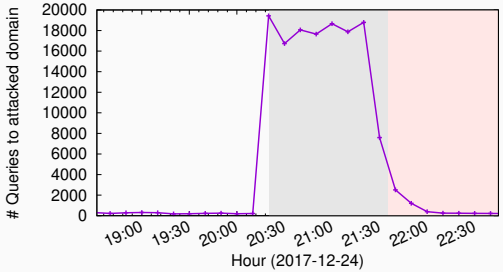

Figure 7: Timeseries of queries to targed domain from Fig. 6.

5 domains likely suffered alongside this targeted domain

Shared hosting: 8 out 319 under attack?

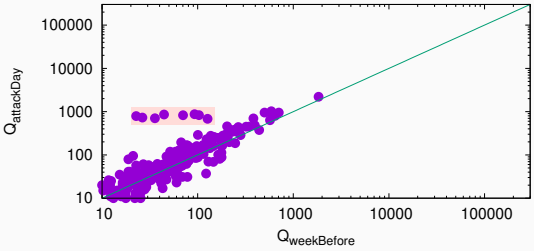

Figure 8: 8 suspicious targets `.nl` domains among 319 domains

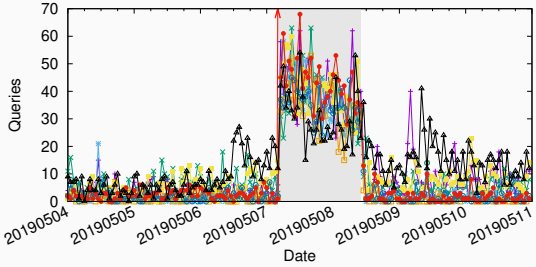

Figure 9: Timeseries of queries to 8 targeted `.nl` domains

- A more coordinated attacked?

Conclusions

- We look into 22 months of attack data from NaWas
- They are not that big (as others have previously shown)
- Neither they last very longitudinal
- We triangulate the data with DNS data:
  - records (OpenIntel)
  - traffic (SIDN's `.nl` Authoritative traffic)
- We show evidence of collateral damage
- And we show different attack strategies on DNS traffic
- Paper: https://tinyurl.com/y5yothlf