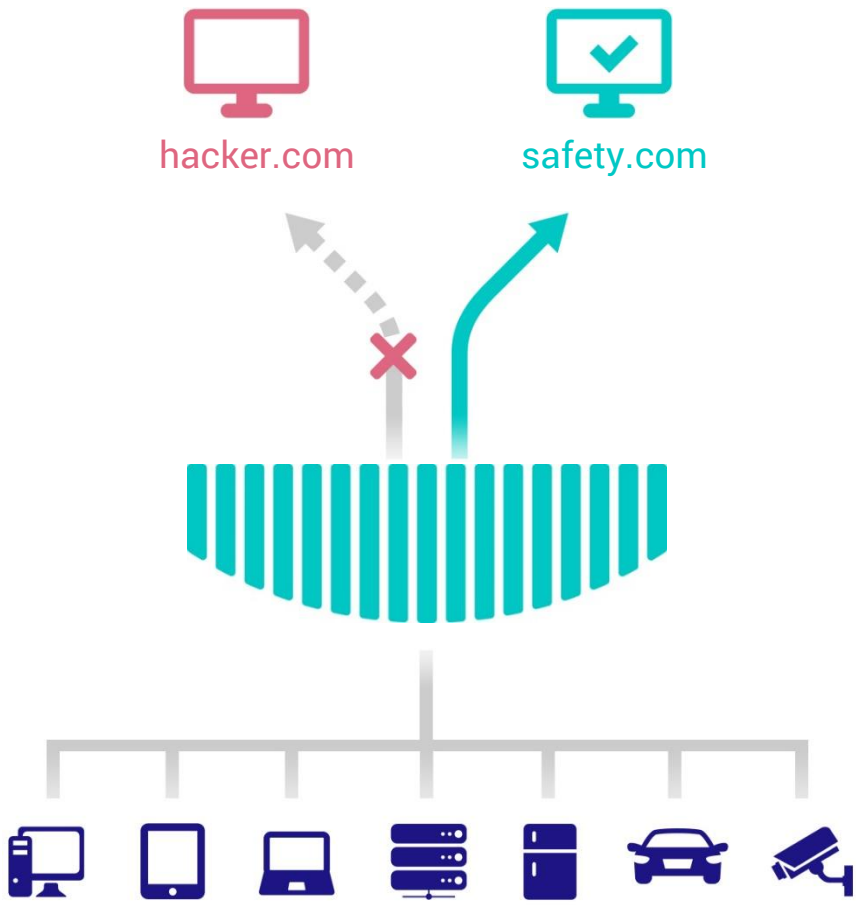
The latest news in the DNS resolution

Based on our own practical experience

- Whalebone provides DNS resolution for millions of people and devices
- Standard compliance, low latency and stability is a must
- Added anti-malware and anomaly detection layer
- Based on Knot Resolver by CZ.NIC



KNOT RESOLVER

Random subdomain attacks

- Also called slow drip attacks

- Targeted domain is attacked through default resolvers for the botnet devices globally
- Generating many queries to random (therefore non-existent) subdomains from the whole botnet will eventually take the domain down
- Eating up the resolver cache and outgoing bandwidth

xyz.ddostarget.com
abc.ddostarget.com
123.ddostarget.com
...

DNSSEC aggressive cache

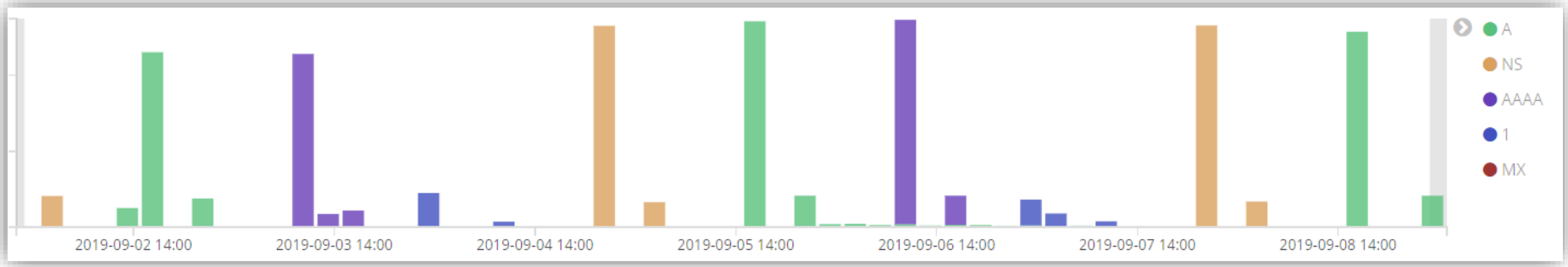
- No need to contact the authoritative server for the proof of non-existence
- No need to cache responses for such non-existent subdomains
- Shielding the authoritative servers (the queries are handled on the resolver)

- Detailed numbers and simulations: DNSSEC aggressive cache (RFC 8198), Petr Špaček (CZ.NIC), https://ripe76.ripe.net/presentations/71-RIPE76-presentation-RFC8198.pdf

Variant of random subdomain attack

Targeted domain: **weaverpublishing.com**

weaverpublishing.com nameserver = ns1.weaverpublishing.com
weaverpublishing.com nameserver = ns2.weaverpublishing.com



mx2.mx2.mx1.mx1.mx1.mx2.mx2.mx1.mx1.mx2.mx1.mx2.mx2.mx2.mta-sts.mx2.mx2.webmail.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mta-sts.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mta-sts.mx2.mx1.mx1.mx1.mx1.mx2.mx1.webdisk.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mta-sts.mx2.mx1.mx1.mx1.mx1.mx2.mx1.webdisk.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx1.mx2.mx2.mta-sts.mx2.mx1.mx2.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx1.mta-sts.mx1.mx2.mx2.mx1.cpanel.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx1.mta-sts.mx1.mx2.mx2.mx1.cpanel.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mta-sts.mx1.mx2.mx2.autodiscover.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mx1.mx2.mta-sts.mx1.mx2.mx2.autodiscover.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx2.mx2.mta-sts.mx2.mx1.mx1.mx1.mx2.mail.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx1.mx2.mx2.mx2.mta-sts.mx1.mx2.mx2.mta-sts.mx2.mx2.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mail.weaverpublishing.com.
mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mx2.mx2.mx2.mx1.mx2.mail.weaverpublishing.com.

Virgin Media's promotional contest as for **Monday 9 September 2019**

Dear client Virgin Media,

we would like to thank you for your loyalty to **Virgin Media**, therefore, we offer you a chance to win a **Samsung Galaxy S10**.

Win a Galaxy S10!

↓ All you have to do is choose the correct gift box ↓

19 821 people like that.

Pauline Collet

I'm so happy that I won!! I've just paid 1£ and now I'm waiting for my new Galaxy to come :)

Reply · Like · 4 minutes ago

DNSSEC aggressive cache - issues

- F5 BIG-IP Load balancer faulty implementation of proof of non-existence
- Query for non-existent record type get NSEC3 response stating that only TXT records exist -> Resolver returns NXDOMAIN for ongoing A records
- Workaround and fix provided by the vendor, still not applied at many organizations
- Issue originally created by Whalebone and analyzed by CZ.NIC https://github.com/dns-violations/dns-violations/blob/master/2018/DVE-2018-0003.md

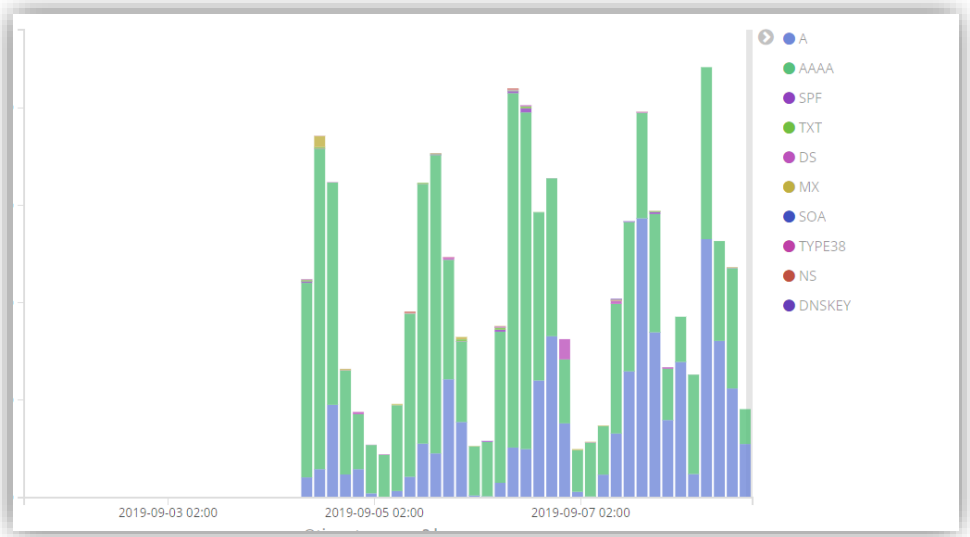
DNSSEC aggressive cache - issues

- F5 BIG-IP balancers are used by banks, government and large service providers
- Issue emerged randomly and disappeared quickly making in very hard to analyze

- Error in DNSSEC implementation on F5 BIG-IP load balancers, Petr Špaček (CZ.NIC), https://en.blog.nic.cz/2019/07/10/error-in-dnssec-implementation-on-f5-big-ip-load-balancers/

DNSSEC validation failures monitoring

1. Domains with expired keys
2. Misconfigured domains (even TLDs!)
3. Attacks?



ISP will always be the first one to blame ☹

.sk DNSSEC deployment

- Overnight TLD DNSSEC deployment with some issues
  - 8 servers with correct configuration
  - 6 misconfigured with wrong proofs
- Resolution randomly ended up in validation failure
- Unreachable domains for end users resulting in ISP helpdesk calls
- Reproduction of the issue unreliable due to majority of correctly configured servers
- Fixed quickly once we called them directly

- Thanks CZ.NIC and DNSViz for identification!

DNSSEC – is it worth the effort?

- We estimate that DNSSEC validation failures are just **0,01% of all DNS queries in our networks**

- **Sign, Validate and Monitor!**

- DNSViz does a great job at analysis:
  - Properly configured DNSSEC: http://dnsviz.net/d/nic.cz/dnssec/
  - DNSSEC issues: http://dnsviz.net/d/szn-broken-dnssec.cz/dnssec/

Filter threats off your network

Robert Šefr, CTO
robert.sefr@whalebone.io
@robcza

https://whalebone.io

whalebone