DNS Security and Privacy: Quad9 Overview

Michael Hausding (SWITCH)
michael.hausding@switch.ch
SwiNOG37 Bern 2.12.2021

SWITCH and Quad9

SWITCH and PCH are founders of the Swiss Quad9 foundation.

SWITCH has a mandate by the Office of Communications to support Quad9 in Switzerland.

SWITCH-CERT is a threat intel provider for Quad9.

Quad9 Mission

Provide security and privacy via DNS-based services to a worldwide audience, at no cost, and with comparative or better performance as existing systems.

Reduce the harm of criminal behavior on the internet that is targeting end users and networks.

Quad9 Mission

- Secondary goals:
  - By providing an example of best practices, compel other organizations to improve their security and privacy stances to match our offering.
  - Improve the stability and performance of the DNS and related infrastructure that is consistent with our primary mission.
  - Assist with protocols and implementations that support our primary mission.
  - Deploy to under-served markets where security & privacy services are limited, which indirectly constrains equality and economic growth

Overview

- Non-profit based in Switzerland
- Started in 2016, public operation since late 2017
- Moved to Switzerland in February 2021
- Small team: less than 10, core staff all with ISP backgrounds
- Founded with support from IBM, Global Cyber Alliance, Packet Clearing House
- Block lists provided by more than 20 security intelligence providers
- No logging, high-privacy - GDPR + Swiss Data Protection laws

How do we survive?

quad9

- Corporate Sponsorship
- Grants and non-profit support
- Donations in-kind
  - Servers
  - Co-location: space, power, transit bandwidth
- Individual support via small-amount donations

Why .ch?

- No national legislation on privacy in US
- Switzerland has extremely rigorous privacy guidelines (criminal + civil)
- Complaints can be brought by anyone, not just Swiss citizens
- No history of secret laws for data collection
- Switzerland has well-defined MLAT interactions and structures
- Switzerland was very high in Corruption Perception Index Score
- Findings of law that placed Quad9 into well-defined industry sectors

DNS Blocking

Blocking on the DNS level should be in line with the users intent and consent

Swiss Law and DNS blocking

quad9

Quad9 was found not to be a provider of telecommunications services, therefore is exempt from regulation under the Federal Act on the Surveillance of Post and Telecommunications (SPTA; SR 780.1)

See https://www.quad9.net/privacy/compliance-and-applicable-law/

DNS Blocking for Security

What we block:

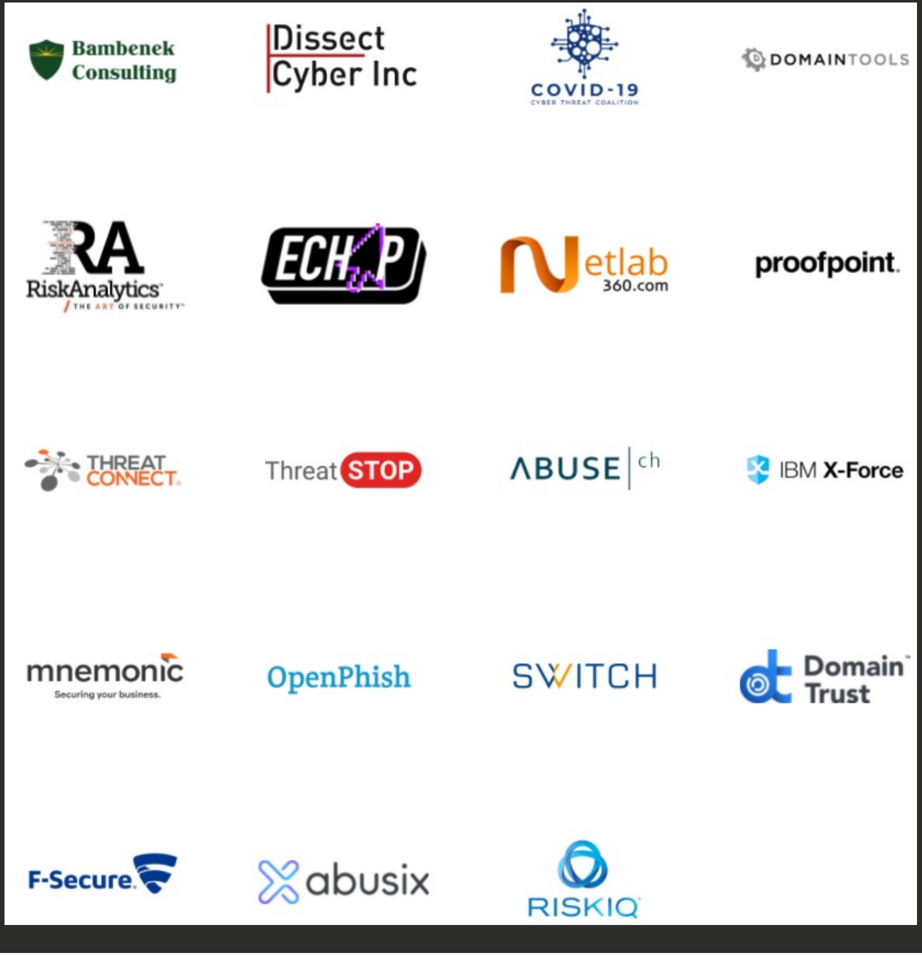
- Malware
- Phishing
- Stalkerware/spyware
- C2 systems / botnets
- Lookalike domains
- Other risks to end users that intend harm

What we do not block:

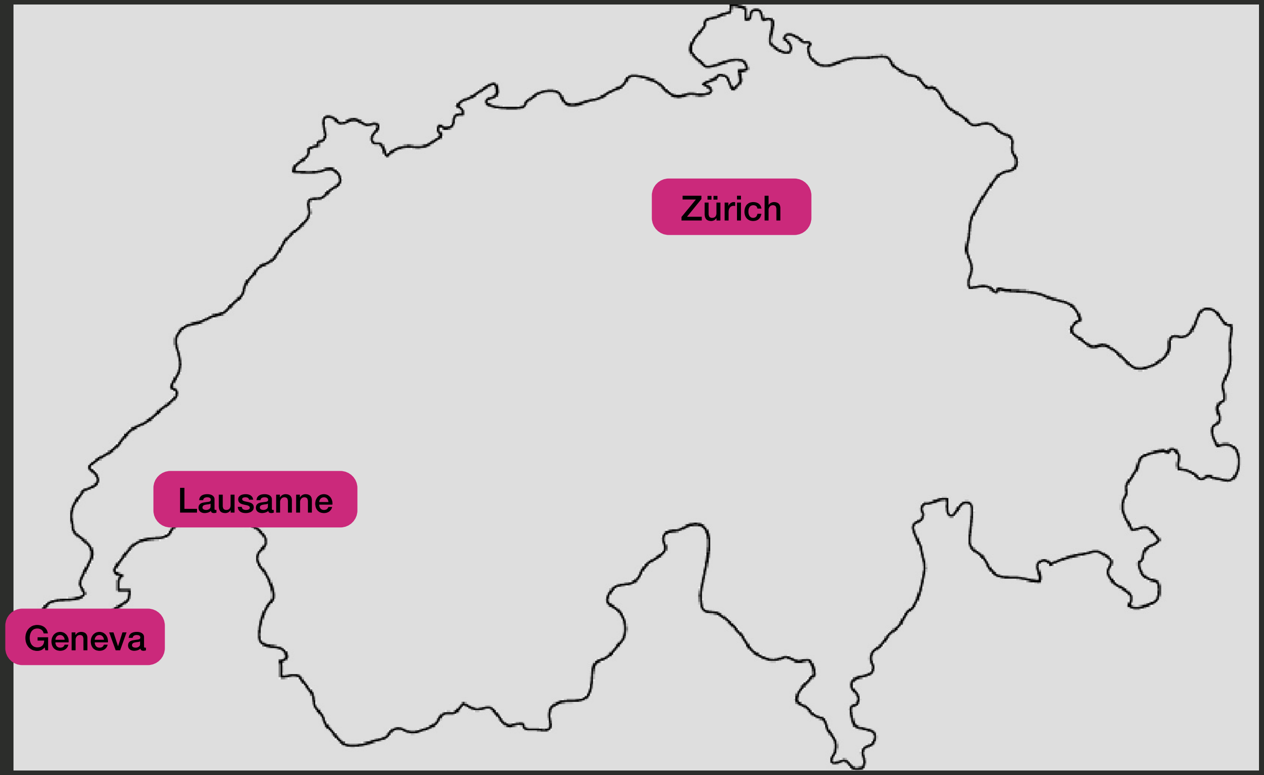
- Content

Threat Intelligence Partners

quad9



Locations in Switzerland



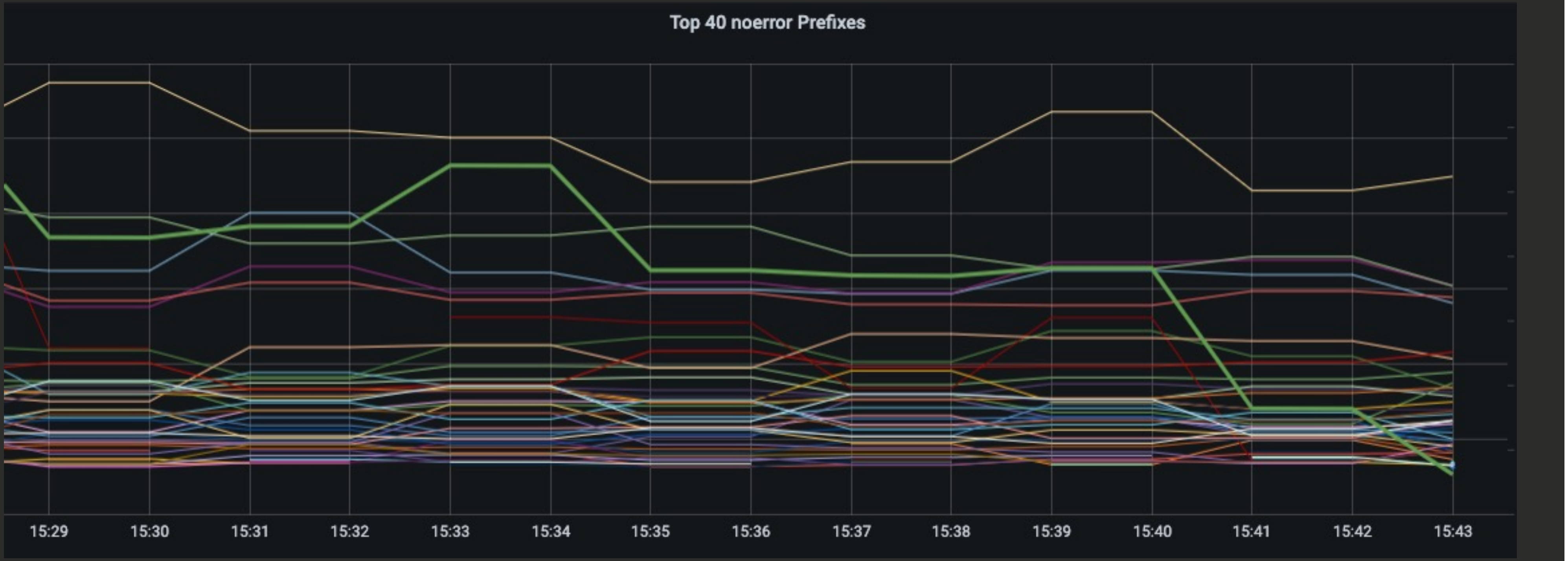
General Deployment

- Multiple layers of redundancy:
  - Anycast: POP-by-POP failover/load management
  - ECMP: server-by-server failover/load management
  - Multiple back-end resolvers: no one resolver is relied upon
  - Multiple back-ends to the back-ends: distribute load back out of POP
- POPs operate autonomously, but with “fail-safes” to prevent cascading faults
- Typically installed in IX locations - strong desire to keep data in-country
- Runs on Cisco UCS systems (M5-off lease)
- 10G ports for interconnect upstream (multiple for big locations)

Software Stack

- Front-end: dnsdist (PowerDNS)
- Back-ends:
  - PowerDNS recursor (PowerDNS)
  - unbound (NLNet Labs)
  - BIND (ISC)
- Ubuntu & CentOS underneath
- Prometheus, Grafana, Kafka, zfs, haproxy, many other OSS applications
- All components are open-source - patches and features contributed back

Monitoring


Top 40 noerror Prefixes
15:29
15:30
15:31
15:32
15:33
15:34
15:35
15:36
15:37
15:38
15:39
15:40
15:41
15:42
15:43

Quad9 for ISPs

- ISPs can use Quad9 for free
- Filtering of malware & phishing is a reason to use Quad9
- Forwarding from own cache is prefered to further enhance privacy & speed
- Please contact us if you have more than 25’000 users
- Quad9 doesn’t filter unlicensed gambling sites as required for ISPs

You can help!

- Sponsorship - funding is highest need now (staffing up)
- New threat intelligence sources of high quality needed
- Server co-location, transit in “edge” networks
- …preferably with hardware included if it meets specifications.
- Blogging, testing, talking to your peers about Quad9
- The more users on the system, the better the privacy and cache freshness

questions?

9.9.9.9 / 149.112.112.112 / 2620:fe::fe

michael.hausding@switch.ch

Bonus: Additional services

- 9.9.9.10 = No blocklist, no DNSSEC
- 9.9.9.11 = Blocklist and ECS (/24 and /56)
- Coming soon: splash page (redirect)

Bonus: Blocking Events - Customer Views

Quad9 has no reporting interface of any kind

- Storage of account data would violate our “no data” rule
- Data collection or reporting is not in line with current mission

HOWEVER…

All NXDOMAIN responses from Quad9 from malicious blocks are tagged. Response bits of recursion_available=0 and authority=0 set on all replies from blocklist.

Bonus: Privacy Extensions

Additional privacy enhancements:

- DoT/DoH/DNSCrypt support
- ECS - strip ECS from “secure” services
- On ECS-enabled services, limit netmask
- qname minimization
- BGP-prefix summarization for volumetric data
- Locality blurring for threat data
- Privacy policy used as the example for RFC8932

Bonus: Threat Intelligence Partners

TI providers receive realtime information on:

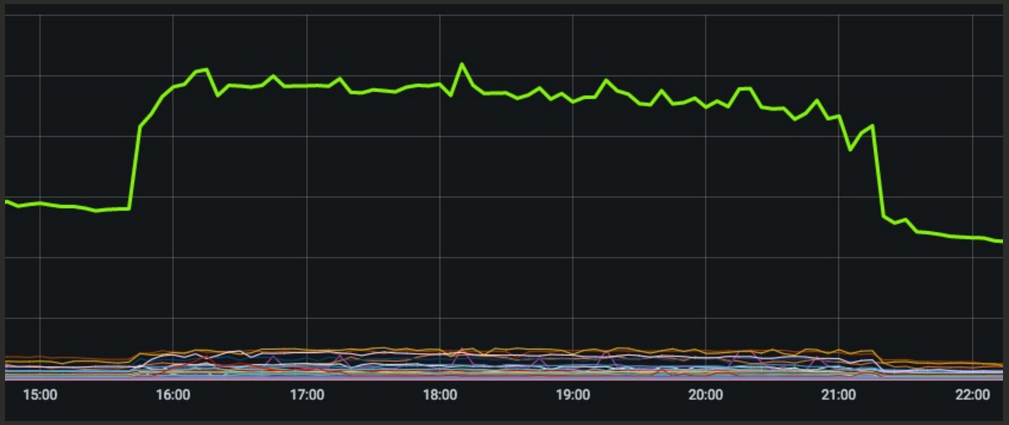
- FQDN of block events based on their provided lists
- Timestamps for evaluating growing/falling threats
- Rough geography of client

Also provided:

- Large customer base reporting of false positives
- New reports of malicious domains reported to Quad9 by end users

Bonus Slide: Facebook outage

- ~80% increase in total QPS; some POPs were >100%
- SERVFAIL traffic was handled by packetcache (dnsdist FTW!)
- No customer complaints; some latency in some POPs
- Technically, our latency dropped significantly since SERVFAIL is fast
- No issues during ramp-up; FB did seem to have rate-limit issues during first few minutes (REFUSED) but that dropped quickly


15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00