

DNS RPZ in the Swiss NREN

First-hand experiences after half a year of productive usage



Matthias Seitz
matthias.seitz@switch.ch

Tallinn, 25th of September 2015

Agenda

- What is DNS RPZ?
- Timeline of the project at SWITCH
- SWITCH RPZs
- Web landing page and its purpose
- Log- and monitoring infrastructure
- A typical work routine
- Success story

DNSfirewall



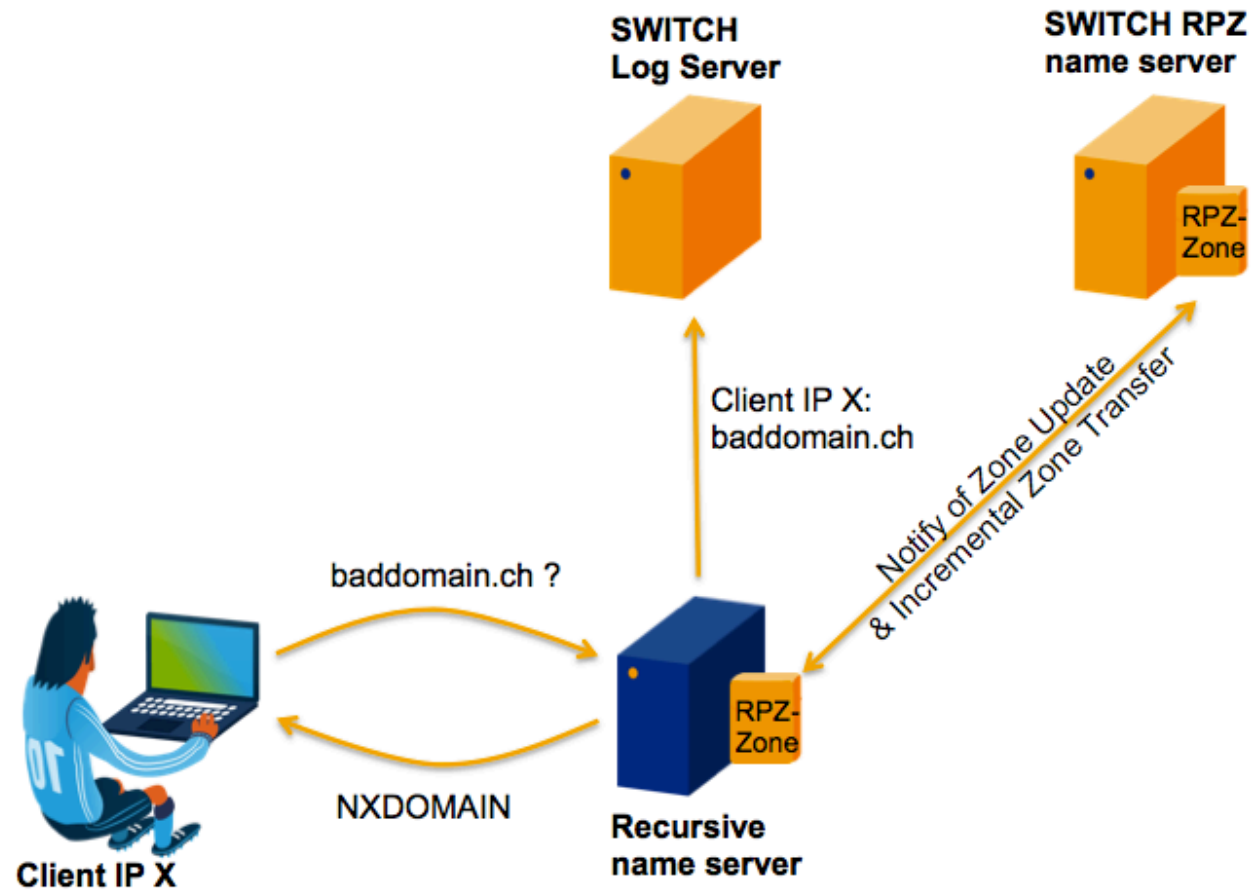
DNS RPZ

- With RPZ, it is possible to control the answering behaviour of a recursive DNS server
 - Firewall on DNS level
- **Response Policy Zone**
 - Domains with policies: allow, drop, log
- A RPZ can be handled as any other DNS zone
 - XFR, NOTIFY, TSIG
 - Propagation is timely, efficient and authentic

DNS RPZ

- Internet security problems:
 - Malware infection sites, drive-by downloads
 - Malware command-and-control, botnet
 - Phishing
 - APT attacks
- Restrict access to malicious domains
- Runs on recursive DNS servers with BIND or on Infoblox devices

DNS with RPZ



DNSfirewall

- Name of the RPZ project / service at SWITCH
- Service includes
 - Zone transfer to institutions. Or the institutions can use the SWITCH resolvers. SWITCH and external RPZs
 - Most-likely infected reports to security contacts at the institutions
 - Web landing page for redirecting and informing the enduser
- Side projects
 - Logging / monitoring infrastructure
 - IOC-DB (database with indicators of compromise)

Timeline

- September 2013: Internal RPZ testing, asking the community for their interest
- February 2014: Trial with three institutions and four zone providers
 - detection and log mechanism works
 - zone transfer from the providers works great
 - transmission of the hits work
 - the setup is reliable
 - **problem: no appropriate zones**

Timeline

- June 2014: Spamhaus introduces splitted RPZs
- Summer 2014: Evaluate log- and monitoring solution
 - Splunk vs ELK
- September 2014: Second trial with Spamhaus and Farsight Security RPZs with two institutions.
 - **Still no appropriate zones**
- December 2014: SURBL introduces splitted RPZs
 - Malware and phishing RPZ

Timeline

- January 2015: Third trial. SURBL is fine against spy- and greyware.
- March 2015: purchase of the SURBL RPZs and decision also to maintain some SWITCH RPZs
- June 2015: first productive customer
- September 2015: Five productive customers
 - 40'000 endusers

SWITCH RPZs

- zone.mw.rpz.switch.ch
 - Automated input from internal analysis of malicious .ch / .li domain
 - DGAs
- zone.ph.rpz.switch.ch
 - Automated input from internal analysis of malicious .ch / .li domain
- zone.misc.rpz.switch.ch
 - Adware, spyware, scams
- zone.wl.rpz.switch.ch
 - Whitelist

zone.mw.rpz.switch.ch

- Contains mainly DGA domains
 - most from external sources
 - About 760'000 DGA domains, changes daily
 - vvvqrsensinaix.com, egrzrsensinaix.com, wufkrsensinaix.com
zzwrrsensinaix.com, jtxtrsensinaix.com, vtkirsensinaix.com,
wuyMrsensinaix.com, bbrqrsensinaix.com
- Malware families
 - About 50 different kind of malwares
 - cryptolocker, dircrypt, dyre, emotet, gozi1m, gozi3m, tinba...

Landing page

- User awareness
- Getting more information
 - URL
- Two landing pages in four languages
 - One for malware and one for phishing
 - German, french, italian and english
 - Index the data monitoring system

Landing page

SWITCH

Warning: Phishing site

Warning

The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a phishing web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.

The refusal of this website was managed by SWITCH-CERT in order of your institution.

Reporting a false positive

If you think a request to a website is wrongfully restricted, please inform SWITCH-CERT. To do that, add the technical information which is shown below to a email, add a short description why the domain should not be on the list anymore and send it to cert@switch.ch

Client: 130.59.27.130
Queried domain: 121usa.com
Queried port: 80
URL: 121usa.com/
Time of access(UTC): 2015-09-23 12:25:38.420

Contact

For further information and support, please contact the IT support of your institution.

SWITCH : cert@switch.ch

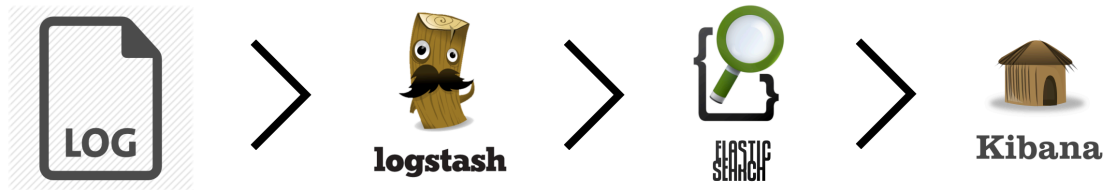
Landing page

Reporting a false positive

If you think a request to a website is wrongfully restricted, please inform SWITCH-CERT. To do that, add the technical information which is shown below to a email, add a short description why the domain should not be on the list anymore and send it to cert@switch.ch

Client:	130.59.27.130
Queried domain:	121usa.com
Queried port:	80
URL:	121usa.com/
Time of access(UTC):	2015-09-23 12:25:38.420

Log- and monitoring infrastructure

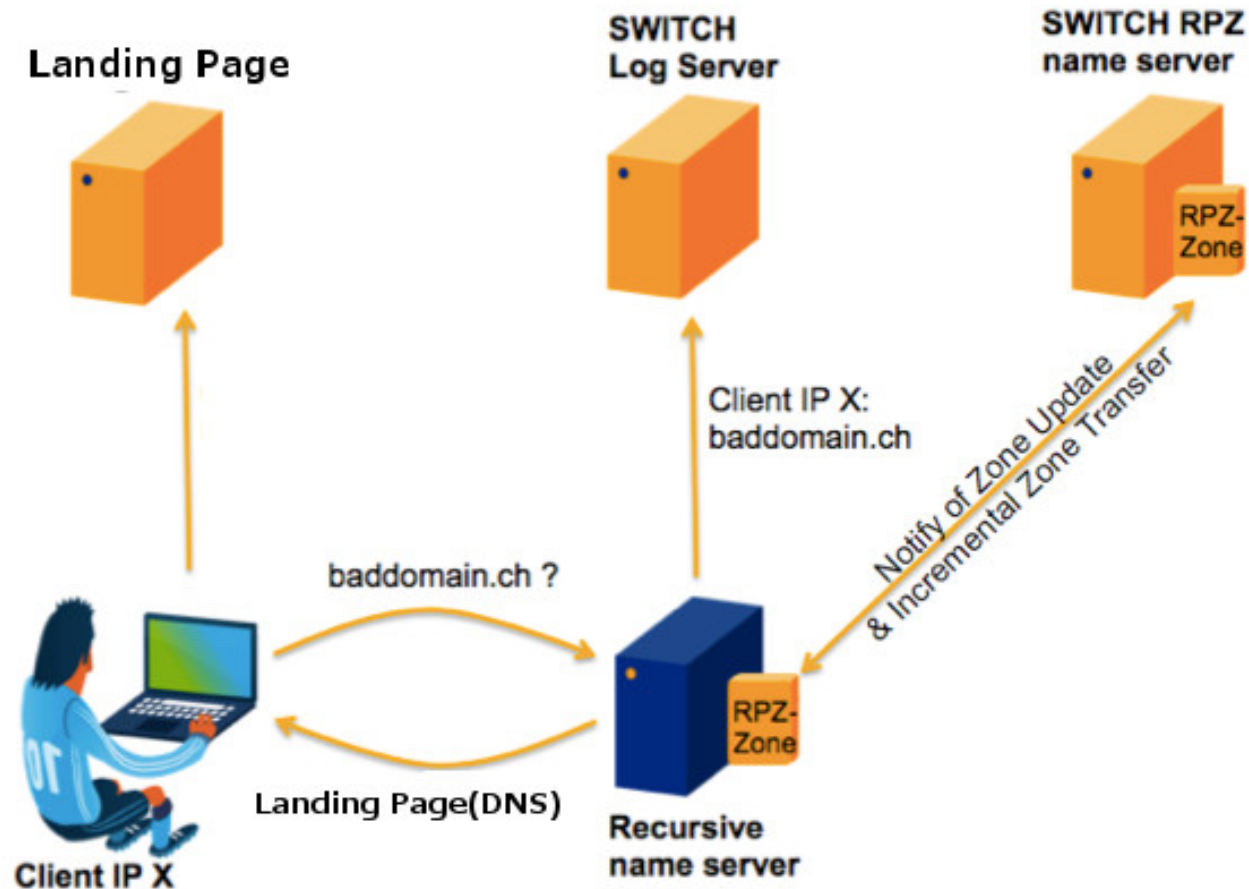


splunk® >

Log- and monitoring infrastructure

- Splunk
 - Easy installation, good documentation, works out of the box
 - expensive
- ELK (**E**lasticsearch, **L**ogstash and **K**ibana)
 - Easy installation, needs time to setup, works out of the box with a limited feature set
 - Opensource, Support also costs money
- Manpower vs money

A typical work routine



Success story

- In production at five institutions
 - Protecting 40'000 endusers
 - Goal: Protect all 400'000 endusers in the SWISS NREN 😊
- Multiple detections and most-likely-reports
 - necurs, gozi, supobox, bedep (trojans)
 - at the moment about 10 reports per month
 - XcodeGhost (malicious iOS applications, C&C server)
- Productive systems, no problems so far

Success story

IT manager of a Swiss University

“The new RPZ service runs very well. With this new service, we have detected several security issues at our institution.

The good thing is, that we now see our IT environment more clear, but of course it also produces more work.”

Next steps

- win more institutions
- develop / find solution for managing the domains
- automate most-likely-reports
- expand logging / monitoring infrastructure
- (BIND feature request)

Further information

- <http://securityblog.switch.ch/2015/05/07/protect-your-network-with-dns-firewall/>
- dnssrpz.info
- matthias.seitz@switch.ch or cert@switch.ch

Questions?