Swiss NREN protection with DNS RPZ

First-hand experiences after one year of productive use

Amsterdam, 19th of April 2016

Matthias Seitz
matthias.seitz@switch.ch
SWITCH security department

- 14 employees
- Runs SWITCH-CERT

Protecting the critical infrastructure of our customers
Typical IT threats

• Malware infection sites, drive-by downloads
• Botnets used for all kind of threats
• Phishing
• APT attacks
• Ransomware
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 custom policies: allow, drop, log

• A RPZ zone can be handled as any other DNS zone
  – XFR, NOTIFY, TSIG
  – Propagation is timely, efficient and authentic
DNS without RPZ

a) IP for malicious site?
b) IP
c) HTTP query
d) Malicious data

Enduser

Malicious site

DNS resolver

© 2016 SWITCH
DNS with RPZ

Enduser

- a) IP for malicious site?
- b) NXDOMAIN / redirect
- c) Redirect to safe site

Safe site

RPZ provider
- Notify of zone updates & incremental zone transfer
- RPZ zones

DNS resolver
- RPZ zones
DNS resolver support for RPZ

• Software
  – ISC BIND >= 9.8.1
  – Knot Resolver (Beta)
  – PowerDNS Recursor (experimental)

• Devices
  – InfoBlox
  – BlueCat
  – EfficientIP

• As a service
  – Verisign
Make or buy?

• Commercial RPZ vendors
  – DissectCyber
  – Fahrsight Security
  – Spamhaus
  – SURBL
  – Internet Identity
  – ThreatStop

• Own RPZs
  – Input from CERT work
    • Malicious .CH and .LI domains
    • Partners
Timeline

• September 2013: The beginning
  – SWITCH internal RPZ testing
  – Contact with NREN community

• February 2014: Trial with three institutions
  – Four RPZ 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 – no content information**
Timeline

• June 2014: Spamhaus introduces splitted RPZs

• Summer 2014: Evaluating log- and monitoring solution
  – Splunk vs ELK

• September 2014: Second RPZ trial
  – Spamhaus and Farsight Security RPZs
  – Still no appropriate zones

• December 2014: SURBL introduces splitted RPZs
  – Malware and phishing RPZ
Timeline

• March 2015: Purchase of the SURBL RPZs
  – Decision to maintain also own SWITCH RPZs
  – SWITCH already has DNS infrastructure, low effort

• June 2015: First productive customer

• April 2016: Established in the Swiss NREN
  – Also None-NREN institutions are interested
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

• Different SWITCH RPZs for customers due to licenses
  – NREN vs. None-NREN
Use Case - Malware
Use Case – Phishing
Report Phishing

Haben Sie ein Phishing E-Mail
Leiten Sie Phishing E-Mails an reports[at]antiphishing[punkt]ch

Haben Sie eine Phishing-Seite
Melden Sie Phishing-Seiten via Web-Formular:

Über antiphishing.ch
antiphishing.ch wird von der Melde- und Analysestelle Informationsseicherung im Land das Bundes betrieben, um der Bevölkerung eine einfache Möglichkeit zu geben, Phishing-Versuche zu melden.
SWITCH RPZs

• zone.mw.rpz.switch.ch
  – Malware data
  – Automated input from internal analysis of malicious .ch / .li domain
  – DGAs

• zone.ph.rpz.switch.ch
  – Phishing data
  – Automated input from internal analysis of malicious .ch / .li domain

• zone.misc.rpz.switch.ch
  – Other malicious data like adware, spyware, scams

And some more..
Landing pages

• User information and awareness
  – NXDOMAIN is not user friendly
  – Domain access is denied because of:..

• Getting more information for further analysis
  – URL

• Different / individual landing pages, multiple languages
  – Malware / Phishing landingpage
  – German, french, italian and english
  – Individual landing pages for institutions
  – Feed the data into the log and monitoring system
Landing pages

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

Query domain: landingpage.ph.rpz.switch.ch
Query port: 80
URL: landingpage.ph.rpz.switch.ch/
Time of access(UTC): 2016-04-18 09:38:05.310

Contact

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

SWITCH : cert@switch.ch
Landing pages

Corporate IT
Security Landingpage: Malware

Warning

The web page you tried to visit may contain or distribute malware.
Access to the web page is refused.

Report false positives
If you think this site is incorrectly blocked, you can report this with the information below and a reason to SWITCH-CERT melden.

Client: 130.59.18.86
Queried domain: landingpage-fhnnw.rpz.switch.ch
Queried port: 80
URL: landingpage-fhnnw.rpz.switch.ch/
Time of access (UTC): 2016-04-18 09:40:18.560
Typ: Malware

Contact
For further information and support, please contact:
FHNNW Corporate IT DNS/Firewall Support

IT-Security
Find further information here:
- FHNNW IT-Security
- SWITCH Safer Internet

© FHNW 2016 Corporate IT Support Powered by SWITCH CERT
Log- and monitoring infrastructure

LOG > logstash > Elastic Search > Kibana

© 2016 SWITCH
Log- and monitoring infrastructure

• Splunk
  – Easy installation, good documentation, works out of the box
  – Expensive

• ELK (Elasticsearch, Logstash and Kibana)
  – Easy installation, needs time to setup, works out of the box with a limited feature set
  – Opensource, Support also costs money

• Manpower vs money
CERT workflow with DNSfirewall

- Enduser
  - a) IP for malicious site?
  - b) Redirect to landing page

- DNS resolver
  - d) HTTP query & response
  - c) RPZ hit

- Log & monitoring system
  - e) URL & more

- Landing pages
  - Notify of zone updates & incremental zone transfer

RPZ provider:
- SWITCH
- SURBL

RPZ zones

Log & monitoring system
Dear Security Team,

The DNSfirewall [1] of SWITCH-CERT has detected a system in your network that makes very suspicious DNS queries. These queries are associated with the trojan Matsnu.

Most likely infected system: [masking]

DNSfirewall log entries:

```
_ time src_ip src_port rpz_src_request
2016-03-23 14:10:51.816 50101 bloombergmyboot.com
2016-03-23 14:10:36.731 58508 catalogdrypaper.com
2016-03-23 14:10:22.640 58871 calibrationng.com
2016-03-23 14:10:07.246 49491 rainlazybarrel.com
2016-03-23 14:09:49.034 55101 poolmarinabarbados.com
2016-03-23 14:09:33.832 49816 cornerbankbachelor.com
2016-03-23 14:09:17.733 55251 methodnebraska.com
2016-03-23 14:09:03.637 57856 californiabite.com
2016-03-23 14:08:49.575 52165 historianboard.com
2016-03-23 14:08:34.491 53486 belkinlocanadian.com
2016-03-23 14:08:19.405 52439 bulletinmanhattan.com
2016-03-23 14:08:07.314 54586 fortunematernity.com
2016-03-23 14:07:54.233 60504 automobilesmsgtr.com
2016-03-23 14:07:41.118 54269 hotelleisureart.com
```

Matsnu is a Trojan horse that opens a back door on the compromised computer and then can perform certain actions based on instructions from a remote server. It also changes certain computer settings.

For more information regarding this malware see [2]

We kindly ask you to take care of this system according to your policy and procedures.

Kind regards,
- Matthias Seitz, SWITCH-CERT
Current status

• In production at 15 institutions
  – Protecting tens of thousands endusers
  – Many NREN institutions are in trial mode

• Many malware detections

• Blocking malware, phishing and other threats in the Swiss NREN
Enduser feedback

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.”