



# SWITCH DNS Firewall Update

FIRST TC Amsterdam 2017

# SWITCH

Matthias Seitz

[matthias.seitz@switch.ch](mailto:matthias.seitz@switch.ch)

Amsterdam, 25<sup>th</sup> April 2017



# Foundation purpose

## Excerpt from the deed of foundation

Berne, 22 October 1987

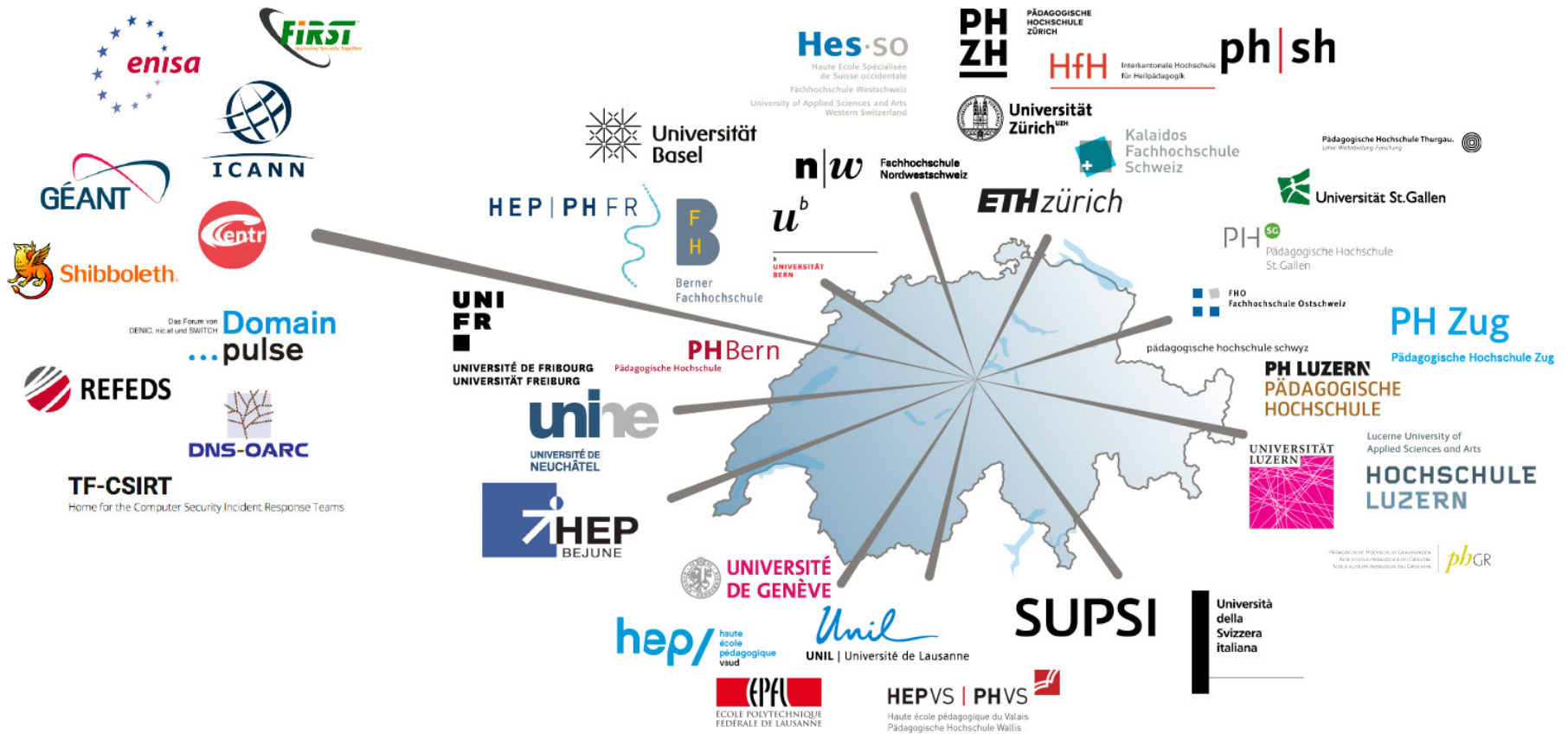


"The foundation has as its objective to create, promote and offer the necessary basis for the effective **use of modern methods of telecomputing in teaching and research in Switzerland**, to be involved in and to support such methods.

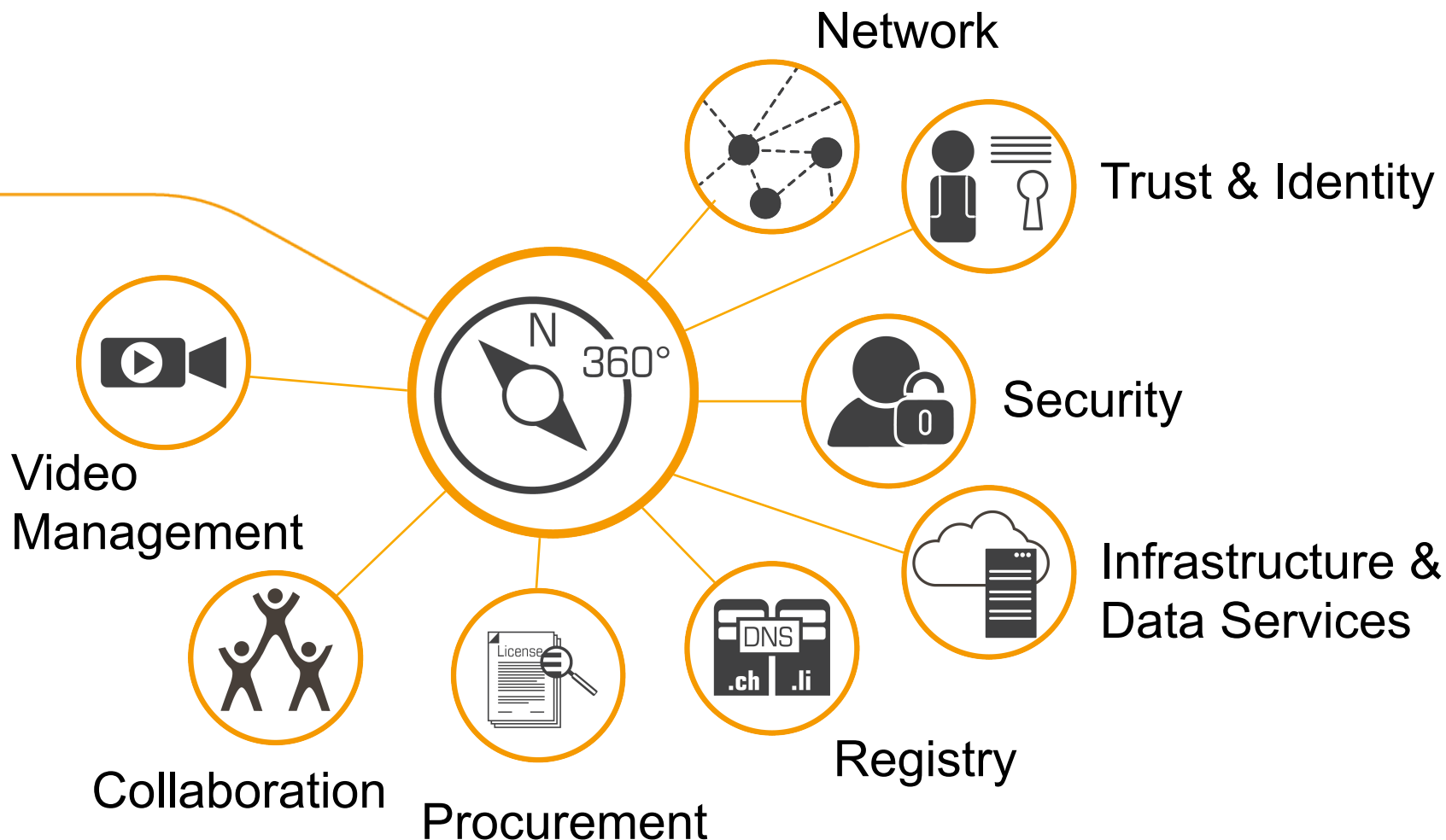
It is a **non-profit foundation** that does not pursue commercial targets."

# International cooperations

# Academic community Switzerland



# Integrated offer



# Our customers



## Higher education

- Cantonal universities
- ETH domain with research institutions
- Universities of applied sciences
- Universities of teacher education

## University-related organizations and administration

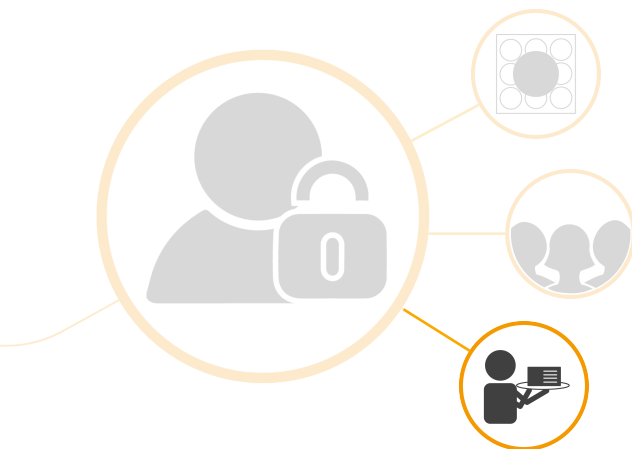
- Hospitals
- Pharmaceutical research

## Commercial customers

- Retail banks
- Cantonal banks and regional banks
- Private banks
- Major banks

# SWITCH-CERT services

20 years SWITCH-CERT –  
information sharing and trusted  
community



- Computer Security Incident Response
- **Network Security Monitoring**
- Trusted Collaboration Services
- **Malware Monitoring & Analysis**
- Malicious Domain Takedown
- Information & Awareness Services
- **DNS for SWITCH / .ch and .li**
- DNS Firewall Service

„DNS Firewall gives you the most bang  
for your buck“

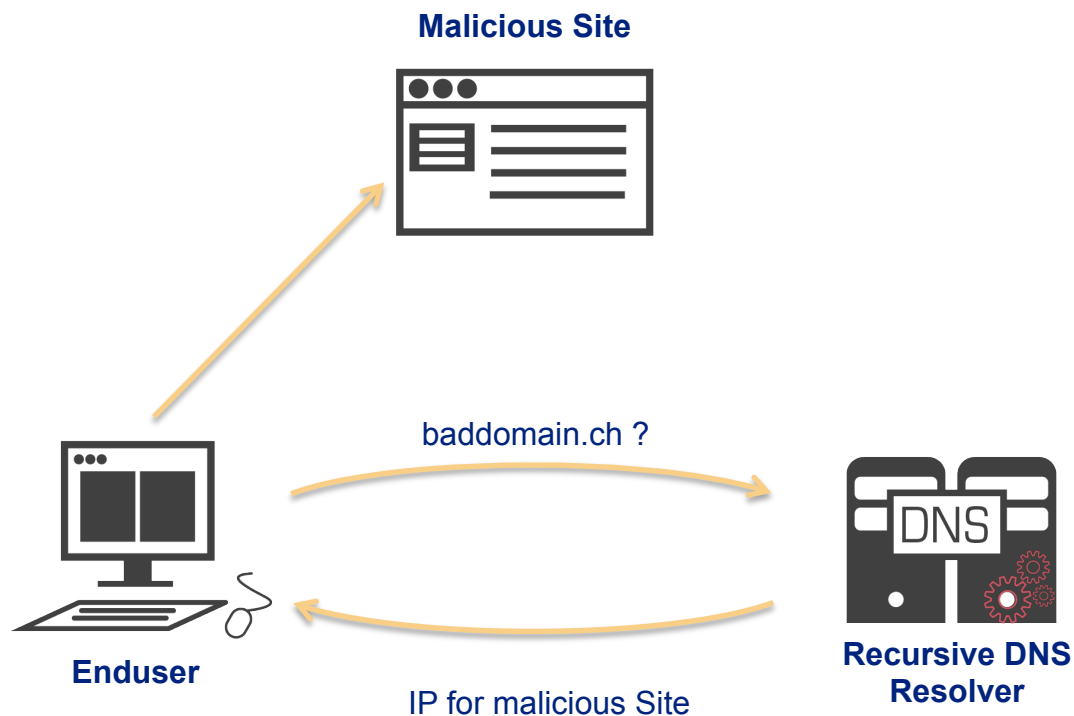
Paul Vixie

# DNS RPZ IETF draft

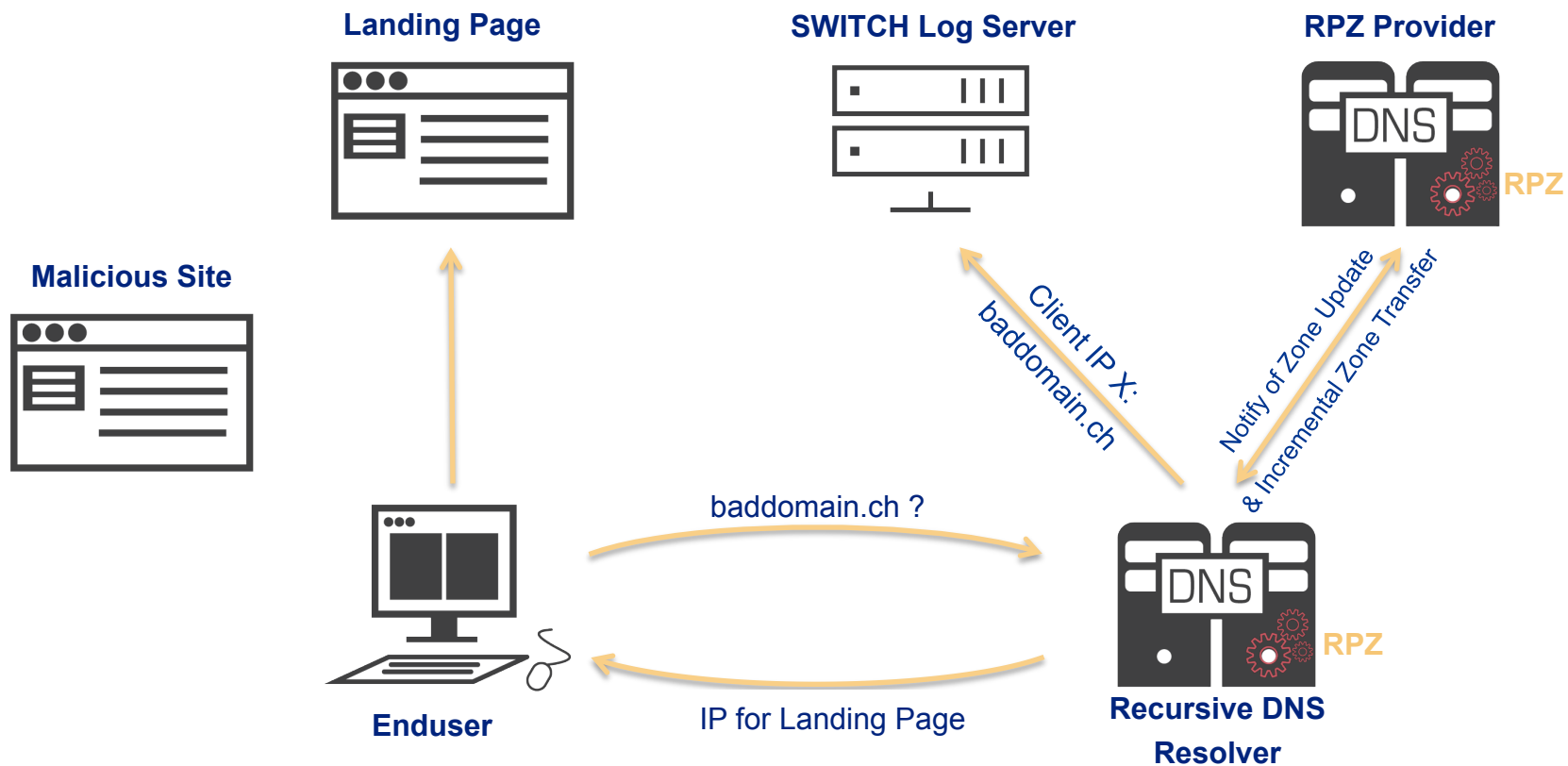
“... method for expressing DNS response policy inside a **specially constructed DNS zone**, and for **recursive name servers** to use such policy to return **modified results to DNS clients**. The modified DNS results can stop access to selected HTTP servers, redirect users to "walled gardens", block objectionable email, and otherwise **defend against attack**. These "DNS Firewalls" are widely used in **fighting Internet crime and abuse**.”



# DNS without RPZ



# DNS with RPZ



# 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](mailto:cert@switch.ch)

**Client:** 2001:620:0:49:5a55  
**Queried domain:** landingpage.ph.rpz.switch.ch  
**Queried port:** 80  
**URL:** landingpage.ph.rpz.switch.ch/  
**Time of access(UTC):** 2017-03-28 13:47:24.371  
**Landingpage:** SWITCH phishing

### Contact

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

SWITCH : [cert@switch.ch](mailto:cert@switch.ch)

# DNS Firewall features

- **Prevention**

- Internal computer infections are prevented by blocking access to infected sites. Data breaches can be prevented.

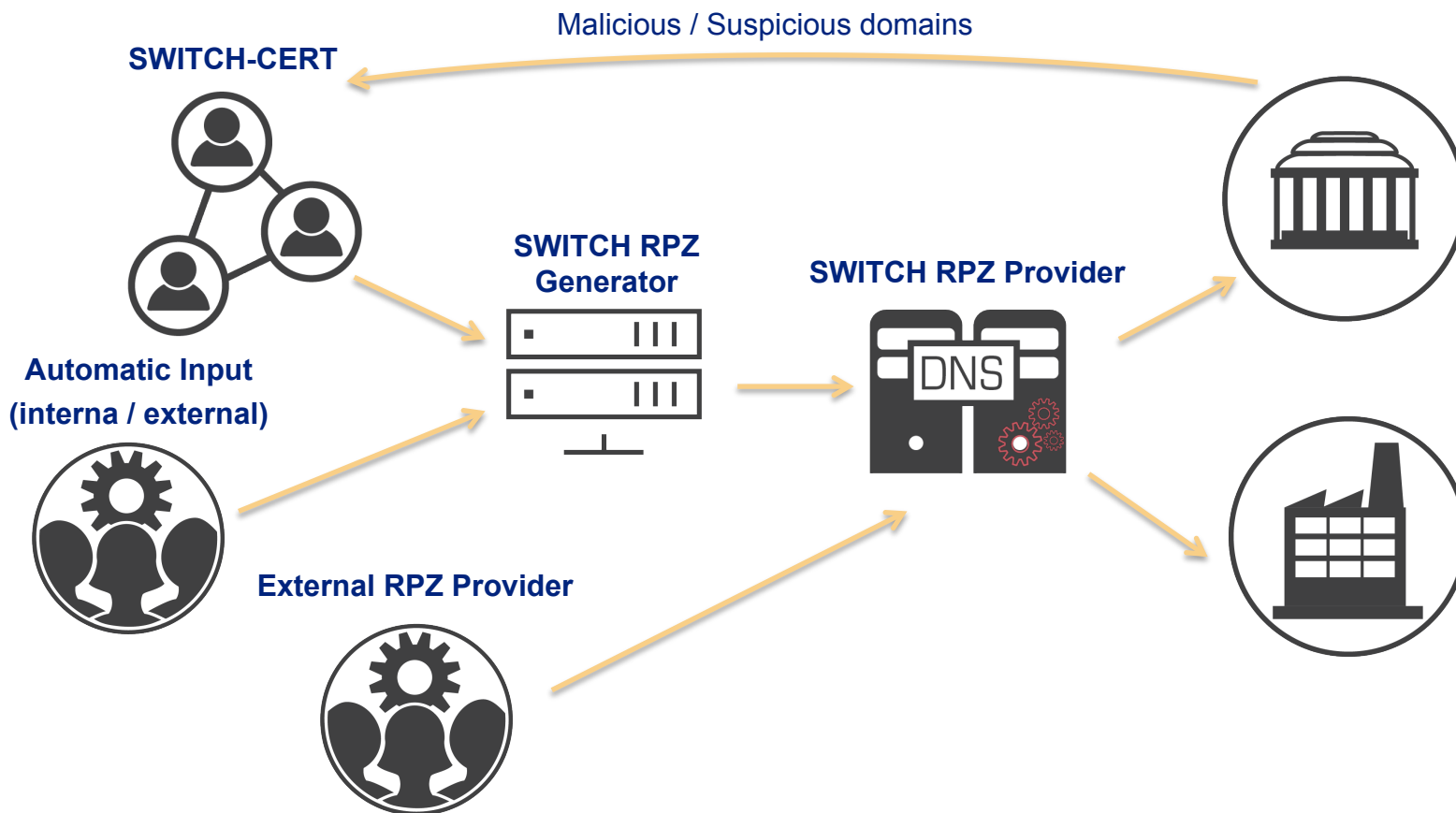
- **Detection**

- SWITCH detects computers that are already infected, and customers are rapidly informed about suspicious and infected computers.

- **Awareness**

- Malicious queries are redirected to a safe landing page that informs the users of the potential risk.

# SWITCH-CERT Threat Intelligence



# Phishing Use Case

- Recommended RPZ policy for phishing: redirect to phishing landing page
- SWITCH maintains an own phishing RPZ
  - Malicious domains from the domain abuse process of .ch / .li
  - National and international data exchange
  - Feedback and reports from customers
- Phishing RPZ from partners


# Report Phishing Domains

SWITCH

Antiphishing Form Privacy Statement

## Report phishing

You can help us fight phishing by using the simple form below to report e-mails. Your report will be analysed by security experts at SWITCH, and measures will be taken to block dangerous websites as soon as possible. Web browsers will get updates of known phishing pages, thus protecting users.



Please report your phishing mail using the form below:

**Sender:** Michael Hausding <michael.hausding@switch.ch> (Information from your AAI login)

**URL:**   
Dangerous URL contained in the phishing mail.  
[Click here to learn how to extract this URL from your e-mail program.](#)

**E-mail:** [Click here to show a box where you can paste in the full e-mail you received.](#)  
(optional)

**Comments:**   
(optional)  
Please tell us if there's something you think we should know.

**Targeted organisation:**   
(if known)  
In case you know the organisation being targeted by this phishing attack, e.g. your own organisation, you can choose it from the list above. Please only select an organisation if you are sure and if it is available in the list.

By clicking on the "Submit" button below, I agree to send the data entered above to SWITCH, together with my AAI login identity. SWITCH will not share this data with third parties, with the exception of the dangerous URL.

Legal notice / Imprint © 2015 for content at SWITCH

# Malware Use Case

- Easiest detection is based on C2 communication (DGA domains)
- Blocking of known malware distributing sites
- Recommended RPZ policy for malware: redirect to malware landing page
- SWITCH maintains an own malware RPZ
  - Malicious domains from the domain abuse process of .ch / .li
  - Ebanking malware with Switzerland as the attack target
  - National and international data exchange
  - Feedback and reports from customers
- Malware RPZ from partners



# Current RPZ provider (draft)

Provider	Data	Origin	Comment
Farsight Security	<ul style="list-style-type: none"><li>Newly observed domains</li></ul>	US	
Spamhaus	<ul style="list-style-type: none"><li>Newly observed domains</li><li>Malicious domains</li></ul>	UK	
SURBL	Malicious domains	CA	
SWITCH	Malicious domains	CH	Focus on Switzerland
ThreatSTOP	Malicious domains	US	

# DNS Firewall as a service 1 (draft)

<b>Provider</b>	<b>Data</b>	<b>Origin</b>
CISCO Umbrella	Malicious domains, DNS tunneling,	US
Comodo Secure DNS	Malicious domains	US
Neustar Recursive DNS	Malicious domains	US
Norton ConnectSafe	Malicious domains	US
OpenDNS Umbrella	Malicious domains	US
Spamhaus DNS Firewall	Malicious domains	UK

# DNS Firewall as a service 2 (draft)

<b>Provider</b>	<b>Data</b>	<b>Origin</b>
SWITCH DNS Firewall	Malicious domains	CH
ThreatSTOP DNS Firewall	Malicious domains	US
Verisign DNS Firewall	Malicious domains	US

# Products that can utilize DNS RPZ (draft)

Product	Comment
BlueCat DNS	
EfficientIP SolidServer	
InfoBlox	
ISC BIND 9	
Knot	Partial support
NLnet Labs Unbound	Patched version available from Farsight Security in exchange of Passive DNS data
PowerDNS Recursor	

# FIRST TC 2016 - One year later

- Ten-thousands of users => Hundred-thousands of users
- Limited to Universities => Also available for commercial customers
- Better internal tools (IOC DB) and processes. Faster reaction on threats.
- Multiple incidents and user feedbacks which are proving that (SWITCH) DNS Firewall is really useful.

# Best practices for RPZ implementation

- Start in **log only mode**, then redirect/block
- Implement **whitelist(s)**
- Setup **landing page(s)**
- Use a **log & monitoring system** (Splunk, ELK, ...)
- Run **long term trials** (60 days+) with different RPZ providers and consider implementing more than one RPZ feed
- **Plan enough time**



# How to become a RPZ provider

- Interesting data, mainly domains
- DNS Know-How and a reliable DNS infrastructure
- Appropriate tools to manage and process the data
- Possibility to propagate your service

# Ressources

<https://tools.ietf.org/html/draft-vixie-dns-rpz-04>

[dnssrpz.info](https://dnssrpz.info)

[swit.ch/dnsfirewall](https://swit.ch/dnsfirewall)



30 Years

SWITCH – an integral part of the Swiss academic community since 1987.

[www.switch.ch/30years](http://www.switch.ch/30years)

