

Swiss NREN protection with DNS RPZ

First-hand experiences after one year of productive use

The logo for SWITCH, featuring the word "SWITCH" in a bold, sans-serif font. The letters "S", "I", "T", "C", and "H" are dark blue, while the "W" is a bright yellow-orange color.

Matthias Seitz
matthias.seitz@switch.ch

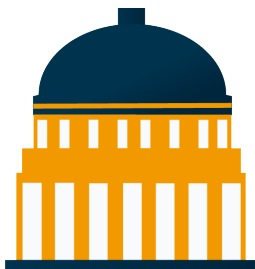
Amsterdam, 19th of April 2016

SWITCH security department

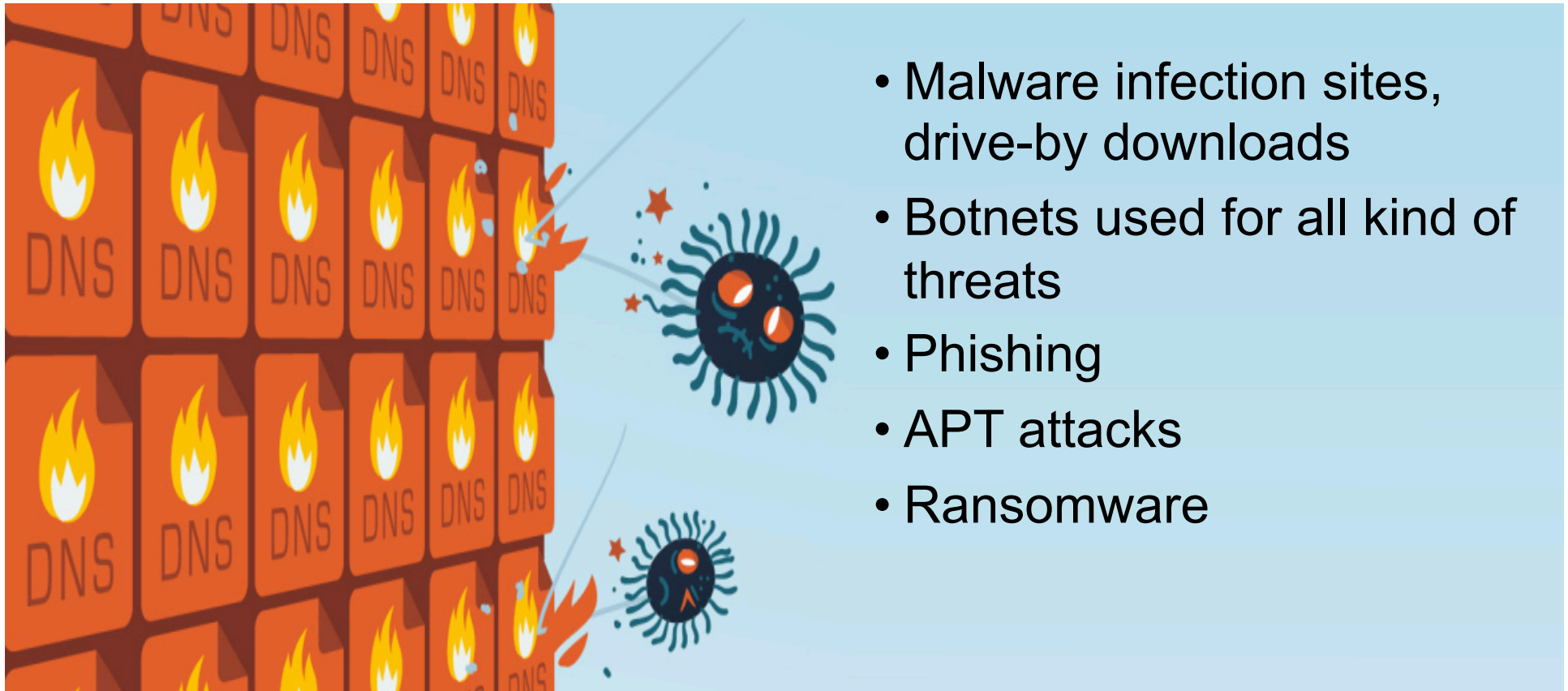
- 14 employees
- Runs SWITCH-CERT



**Protecting the critical infrastructure of
our customers**



Typical IT threats

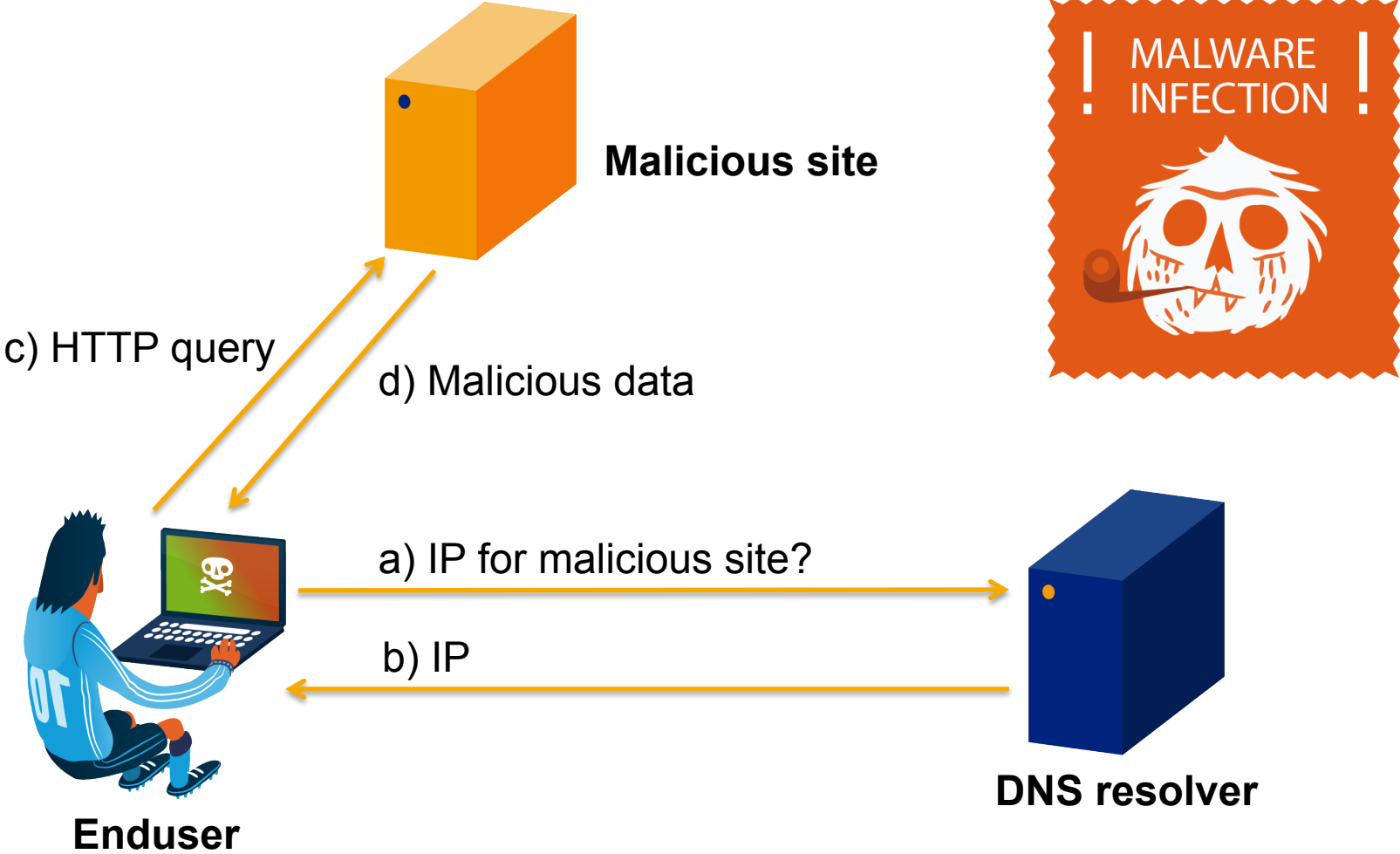


- Malware infection sites, drive-by downloads
- Botnets used for all kind of threats
- Phishing
- APT attacks
- Ransomware

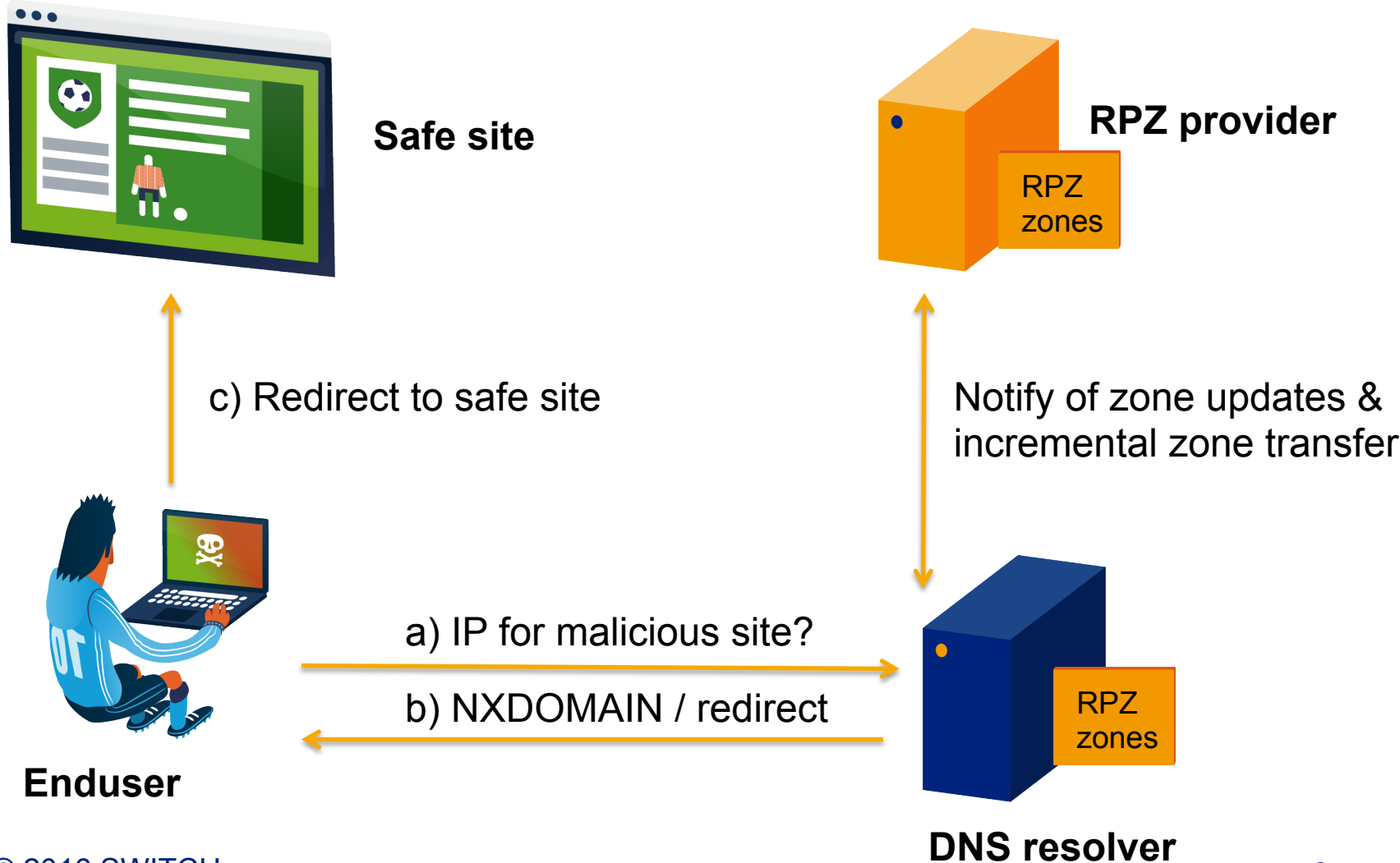
DNS RPZ

- With RPZ, it is possible to control the answering behaviour of a recursive DNS server
 - Firewall on DNS level
- **R**esponse **P**olicy **Z**one
 - 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



DNS with RPZ

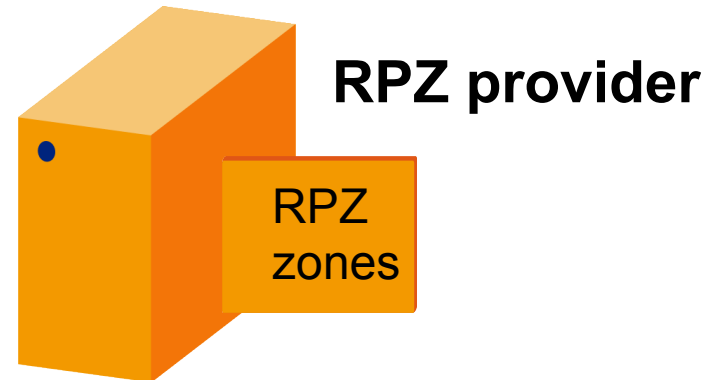


DNS resolver support for RPZ

- Software
 - ISC BIND \geq 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

DNFirewall

- 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

The screenshot displays the antiphishing.ch website. On the left, there is a header with a blue background and a fountain pen. Below it, there are flags for Germany, France, Italy, and the UK. The main heading is "Haben Sie ein Phishing E-Mail" followed by "Leiten Sie Phishing E-Mails an reports[at]antiphishing[punkt]ch". Below this is another heading "Haben Sie eine Phishing-Seite" and "Melden Sie Phishing-Seiten via Web-Formular:". A light blue input field contains the text "URL...". At the bottom left, there is a section titled "Über antiphishing.ch" with a short description of the service.

On the right, there is a red navigation bar with the "SWISS INTERNET SECURITY ALLIANCE" logo and menu items: "Check", "Feedback", "Information", "News", "About us", and flags for Germany, France, and the UK. Below the navigation bar is a "Feedback" section with the text: "You can report suspicious Internet content on this page. Your report will be automatically checked, and we will then take the required steps. Please note you will not receive any feedback. For specific or individual messages, please use the form at the very bottom. Many thanks for your assistance!". Below this is a "Suspicious e-mails" section with a sub-heading "Report suspicious e-mails/Phishing". This section contains the instruction: "Save the suspicious e-mail either in an .eml or .msg format, and then upload it here." It features an "Upload phishing e-mail:" label, a "Choose File" button, and the text "No file chosen". Below this is a question "What's the result 3+4=?" with an empty input field. A "Send" button is located at the bottom of this form.

(optional)

Please tell us if there's something you think we should know.

Optional

Optional: Choose an organization name from the list below, or leave empty.

SWITCH RPZs

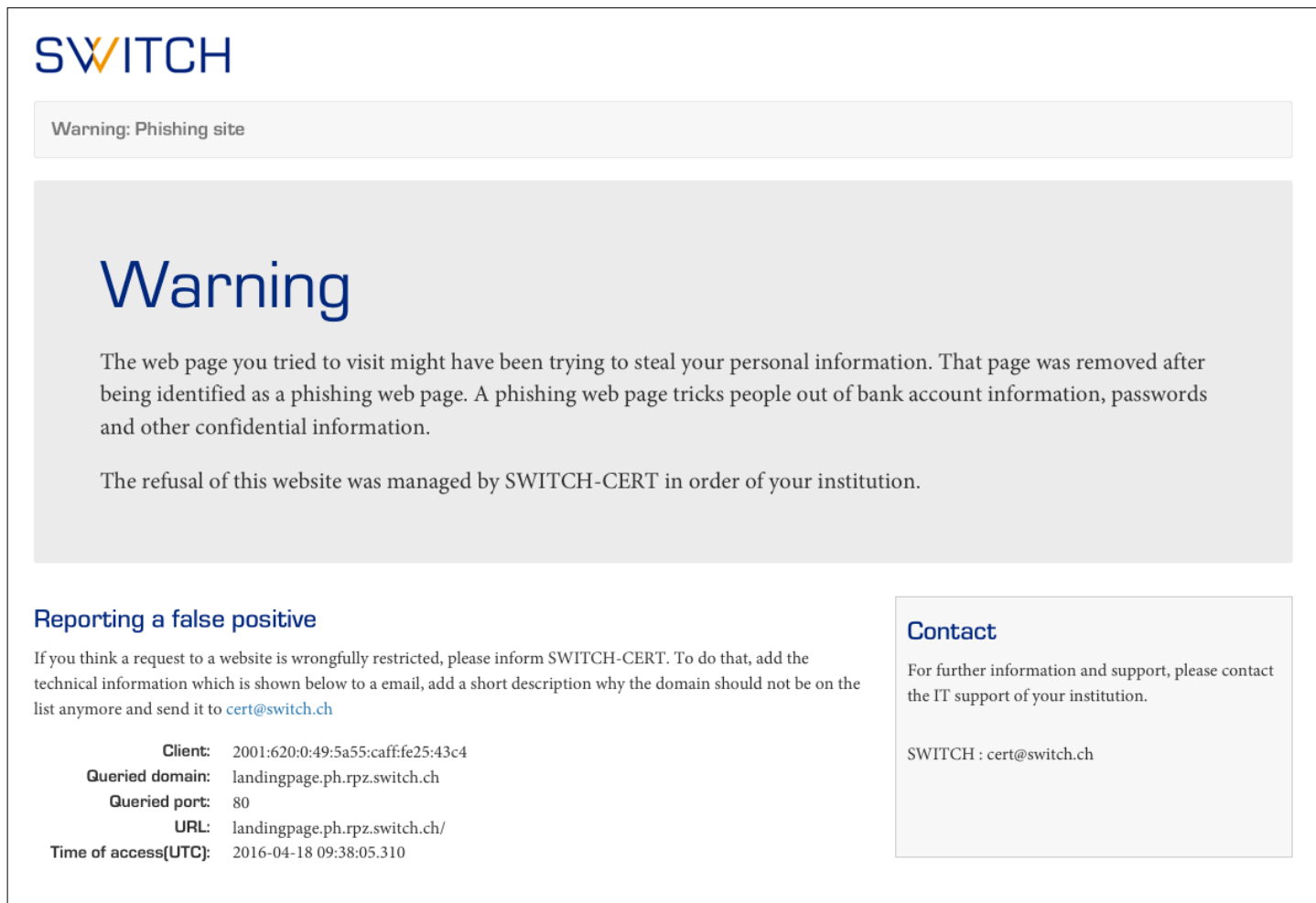
- **zone.mw.rpz.switch.ch**
 - Malware data
 - Automated input from internal analysis of malicious .ch / .li domain
 - DGAs
- **zone.ph.rpz.switch.ch**
 - Phishing data
 - Automated input from internal analysis of malicious .ch / .li domain
- **zone.misc.rpz.switch.ch**
 - Other malicious data like adware, 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



The screenshot shows a web page with the SWITCH logo at the top left. Below the logo is a grey box with the text "Warning: Phishing site". The main content area has a large "Warning" heading, followed by a paragraph explaining that the page might have been trying to steal personal information and was removed. Below this is another paragraph stating that the refusal was managed by SWITCH-CERT. At the bottom left, there is a section titled "Reporting a false positive" with instructions on how to report a wrongly restricted website. To the right of this is a "Contact" section with information on how to reach SWITCH-CERT for further support. Technical details of the access are listed at the bottom left.

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: 2001:620:0:49:5a55:caff:fe25:43c4
Queried domain: landingpage.ph.rpz.switch.ch
Queried 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

n|w Fachhochschule
Nordwestschweiz

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

Contact

For further information and support, please contact:
[FHNW Corporate IT DNSfirewall Support](#)

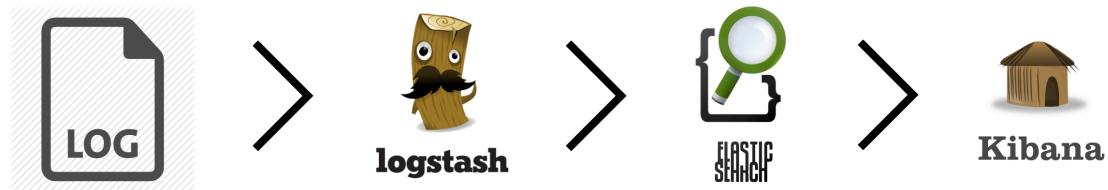
IT-Security

Find further information here:

- [FHNW IT-Security](#)
- [SWITCH Safer Internet](#)

© FHNW 2016 Corporate IT Support Powered by SWITCH CERT

Log- and monitoring infrastructure

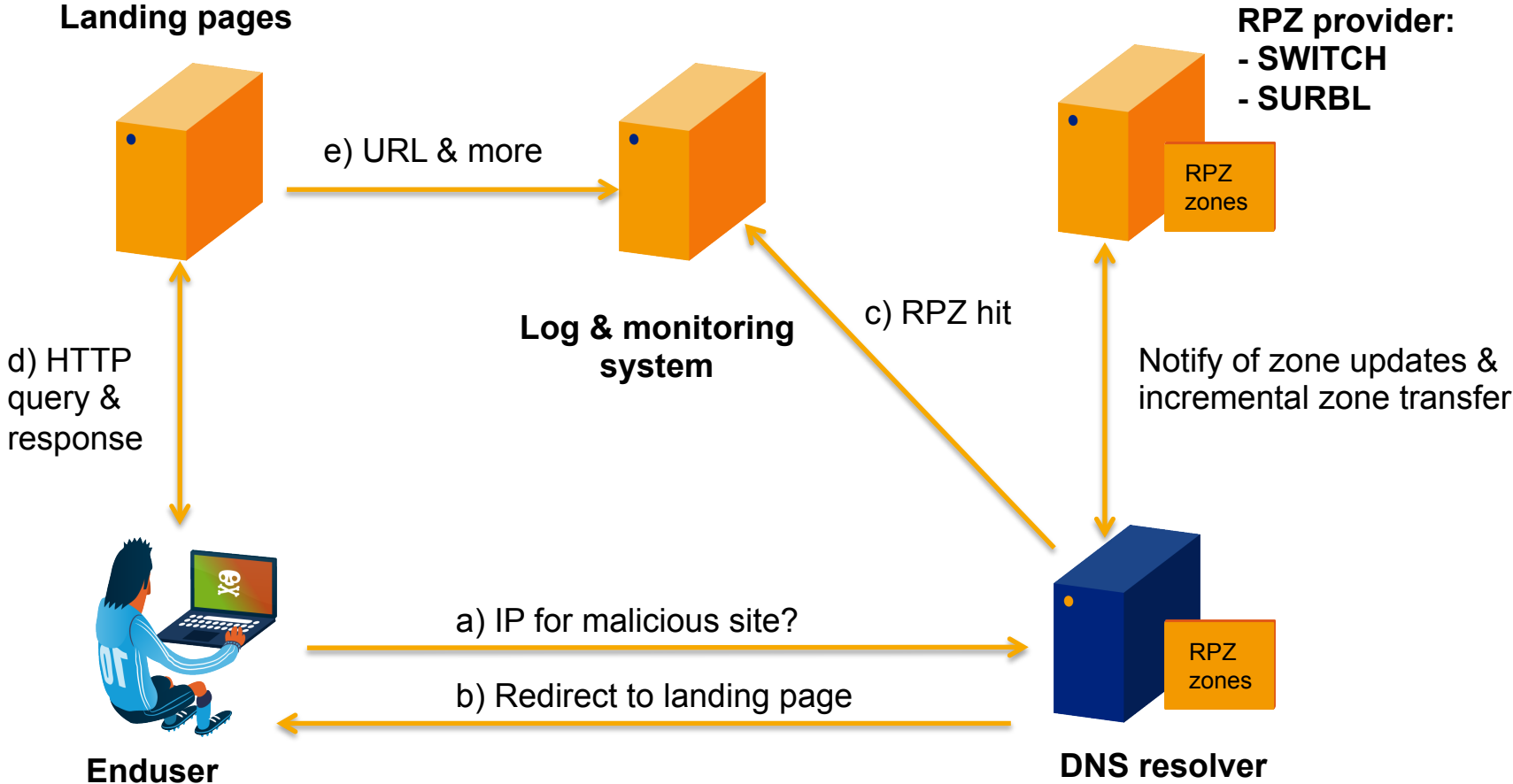


splunk® >

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

CERT workflow with DNSfirewall



Reporting

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: [REDACTED]

DNSfirewall log entries:

_time	src_ip	src_port	rpz_src_request
2016-03-23 14:10:51.816	[REDACTED]	50101	bloombergmyboot.com
2016-03-23 14:10:36.731	[REDACTED]	58508	catalogsdrypaper.com
2016-03-23 14:10:22.640	[REDACTED]	58871	calibrationng.com
2016-03-23 14:10:07.246	[REDACTED]	49491	rainlazybarrel.com
2016-03-23 14:09:49.034	[REDACTED]	55101	poolmarinabarbados.com
2016-03-23 14:09:33.832	[REDACTED]	49816	cornerbankbachelor.com
2016-03-23 14:09:17.733	[REDACTED]	55251	methodnebraska.com
2016-03-23 14:09:03.637	[REDACTED]	57856	californiabite.com
2016-03-23 14:08:49.575	[REDACTED]	52165	historianboard.com
2016-03-23 14:08:34.491	[REDACTED]	53496	belkinlocanadian.com
2016-03-23 14:08:19.405	[REDACTED]	52439	bulletmanhattan.com
2016-03-23 14:08:07.314	[REDACTED]	54586	fortunematernity.com
2016-03-23 14:07:54.233	[REDACTED]	60504	automobilesmgstr.com
2016-03-23 14:07:41.118	[REDACTED]	54259	holeleisureart.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 insitutions 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.”



<http://securityblog.switch.ch>

 [@switchcert](https://twitter.com/switchcert)