SWITCH DNS Firewall Update
FIRST TC Amsterdam 2017

Matthias Seitz
matthias.seitz@switch.ch

Amsterdam, 25th 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

Network

Trust & Identity

Security

Infrastructure & Data Services

Registry

Procurement

Collaboration

Video Management
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
“... 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

Malicious Site

Enduser

Recursive DNS Resolver

IP for malicious Site

baddomain.ch ?
DNS with RPZ

Landing Page

SWITCH Log Server

RPZ Provider

Recursive DNS Resolver

Malicious Site

Enduser

baddomain.ch

IP for Landing Page

baddomain.ch ?

Client IP: baddomain.ch

Notify of Zone Update & Incremental Zone Transfer
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 an email, add a short description why the domain should not be on the list anymore and send it to cert@switch.ch

Client: 2001:6200:49:5a55
Queried domain: landingpage.ph.rpz.switch.ch
Queried port: 80
URL: landingpage.ph.rpz.switch.ch/
Landingpage: SWITCH phishing

Contact

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

SWITCH : 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.
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

Report phishing
You can help us fight phishing by using the simple form below to report emails. Your report will be analyzed 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 Handling
URL: e.g. http://www.example.com/your acción.php
E-mail: (optional)
Comments: (optional)
Targeted organization: (if known)

By clicking 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.

Submit

© 2017 SWITCH | 15
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)

<table>
<thead>
<tr>
<th>Provider</th>
<th>Data</th>
<th>Origin</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Farsight Security</td>
<td>• Newly observed domains</td>
<td>US</td>
<td></td>
</tr>
<tr>
<td>Spamhaus</td>
<td>• Newly observed domains</td>
<td>UK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Malicious domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SURBL</td>
<td>Malicious domains</td>
<td>CA</td>
<td></td>
</tr>
<tr>
<td>SWITCH</td>
<td>Malicious domains</td>
<td>CH</td>
<td>Focus on Switzerland</td>
</tr>
<tr>
<td>ThreatSTOP</td>
<td>Malicious domains</td>
<td>US</td>
<td></td>
</tr>
</tbody>
</table>
## DNS Firewall as a service 1 (draft)

<table>
<thead>
<tr>
<th>Provider</th>
<th>Data</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO Umbrella</td>
<td>Malicious domains, DNS tunnneling,</td>
<td>US</td>
</tr>
<tr>
<td>Comodo Secure DNS</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>Neustar Recursive DNS</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>Norton ConnectSafe</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>OpenDNS Umbrella</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>Spamhaus DNS Firewall</td>
<td>Malicious domains</td>
<td>UK</td>
</tr>
</tbody>
</table>
# DNS Firewall as a service 2 (draft)

<table>
<thead>
<tr>
<th>Provider</th>
<th>Data</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWITCH DNS Firewall</td>
<td>Malicious domains</td>
<td>CH</td>
</tr>
<tr>
<td>ThreatSTOP DNS Firewall</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>Verisign DNS Firewall</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
</tbody>
</table>
### Products that can utilize DNS RPZ (draft)

<table>
<thead>
<tr>
<th>Product</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCat DNS</td>
<td></td>
</tr>
<tr>
<td>EfficientIP SolidServer</td>
<td></td>
</tr>
<tr>
<td>InfoBlox</td>
<td></td>
</tr>
<tr>
<td>ISC BIND 9</td>
<td></td>
</tr>
<tr>
<td>Knot</td>
<td>Partial support</td>
</tr>
<tr>
<td>NLnet Labs Unbound</td>
<td>Patched version available from Farsight Security in exchange of Passive DNS data</td>
</tr>
<tr>
<td>PowerDNS Recursor</td>
<td></td>
</tr>
</tbody>
</table>
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

dnsrpz.info
swit.ch/dnsfirewall
SWITCH – an integral part of the Swiss academic community since 1987.

www.switch.ch/30years