SWITCH DNS Firewall
IMF Conference 2018

Matthias Seitz
matthias.seitz@switch.ch

Hamburg, 7th of May 2018
SWITCH / SWITCH-CERT in a nutshell

• Non-profit foundation, Switzerland, 100 employees

• Swiss NREN: 400‘000 people (Students, staff and researchers)
  • Academic backbone, security, identity management, cloud services, ...

• Registry for Switzerland (.ch) and Liechtenstein (.li)

• SWITCH-CERT: 15 people
  • Security for Universities, e.g. Monitoring like Netflow, DNS Firewall and awareness
  • Operates the DNS name servers for .ch / .li and security service for the registry
  • Security for Banks, specialised in E-banking security; malware analysis
  • Security for other customer groups: Industry and logistic, …
„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

Enduser

Malicious Site

Recursive DNS Resolver

baddomain.ch?

IP for malicious Site
DNS with RPZ

Landing Page

SWITCH Log Server

RPZ Provider

Malicious Site

Enduser

Recursive DNS Resolver

IP for Landing Page

baddomain.ch

baddomain.ch ?

Client IP X: baddomain.ch

Notify of Zone Update & Incremental Zone Transfer

© 2018 SWITCH | 6
Warning

The website you've tried to visit is marked as malicious. It tries to inflict harm to your personal computer, e.g. by installing unwanted software such as adware.

Your institution is using a filter and therefore the harmful requests are redirected to this landing page.

For further information and support, please contact the IT support of your institution. For general information about Drive-by and Internet Threats, consult the SWITCH Safer Internet Website.

SWITCH has two roles in this process. Firstly, in providing information to the institutions about domains that are involved in malicious activities. Secondly, is providing this 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**: 2001:620:
- **Queried domain**: epicunitscan.info
- **Queried port**: 80
- **URL**: epicunitscan.info/
- **Time of access (UTC)**: 2018-03-05 13:26:11.010
- **Landingpage**: SWITCH misc

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 inform the users of the potential risk.
## DNS RPZ Zones files provided by SWITCH

<table>
<thead>
<tr>
<th>RPZ zone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone.mw.rpz.switch.ch</td>
<td>C2, driveby, distribution and other malicious domains. Updates multiple time an hour.</td>
</tr>
<tr>
<td>zone.ph.rpz.switch.ch</td>
<td>Phishing domains, updated every few minutes</td>
</tr>
<tr>
<td>zone.misc.rpz.switch.ch</td>
<td>Malicious domains which are not phishing and not really fit into the malware RPZ.</td>
</tr>
<tr>
<td>zone.wl.rpz.switch.ch</td>
<td>Whitelist, for fast reaction to handle false positives or collateral damage domains from SURBL</td>
</tr>
<tr>
<td>zone.test.rpz.switch.ch</td>
<td>To evaluate new data</td>
</tr>
</tbody>
</table>
Examples and use cases from daily CSIRT operation
Detection and Reporting

- Malicious Site
  - Landing Page
  - Enduser
  - IP for Landing Page

- SWITCH Log Server
  - baddomain.ch?

- RPZ Provider
  - Notify of Zone Update
  - Client IP X: baddomain.ch

- Recursive DNS Resolver
  - IP for Landing Page
  - baddomain.ch
  - RPZ
Detection and Reporting

Information Site
<table>
<thead>
<tr>
<th>_time</th>
<th>src_ip</th>
<th>src_port</th>
<th>cert_dnsrpz_rewrite_query</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-05-05 07:20:01.805</td>
<td>56042</td>
<td>nriel.org</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 07:20:01.805</td>
<td>56042</td>
<td>apwryqobpw.info</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 07:20:01.804</td>
<td>56042</td>
<td>qavayypfs.info</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:46.683</td>
<td>56042</td>
<td>eizau.ws</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:46.683</td>
<td>56042</td>
<td>eizau.ws</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.455</td>
<td>37832</td>
<td>pbgfcwyh.info</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.443</td>
<td>37832</td>
<td>jmaxdnrsl.com</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.443</td>
<td>37832</td>
<td>gtuvizrflo.net</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.443</td>
<td>37832</td>
<td>kcnd.com</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.442</td>
<td>37832</td>
<td>mzicmwfke.net</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.435</td>
<td>37832</td>
<td>tgwoe.biz</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.430</td>
<td>37832</td>
<td>jofnnje.cc</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.418</td>
<td>37832</td>
<td>tvlmxbhlvtv.org</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:47.418</td>
<td>37832</td>
<td>abauctwuqv.org</td>
<td></td>
</tr>
<tr>
<td>2017-05-05 04:16:42.411</td>
<td>37832</td>
<td>apwryqobpw.info</td>
<td></td>
</tr>
</tbody>
</table>
[Detection] Leaking onion domains

2018-04-11T14:54:54, (Client), 53042, hpaur4rufcjojhrag.onion, (Org), Retefe
2018-04-11T14:55:34, (Client), 53203, hpaur4rufcjojhrag.onion, (Org), Retefe
2018-04-11T14:54:57, (Client), 63966, hpaur4rufcjojhrag.onion, (Org), Retefe
2018-04-11T15:10:39, (Client), 54450, hpaur4rufcjojhrag.onion, (Org), Retefe
2018-04-11T16:16:09, (Client), 52356, hpaur4rufcjojhrag.onion, (Org), Retefe
2018-04-11T16:16:17, (Client), 53049, hpaur4rufcjojhrag.onion, (Org), Retefe
[Prevention] Retefe Malware

From Valiant <info@fase.ch>

Subject Ihre Valiant Konto

To Me

Date Mon, 8 May 2017 15:29:03 +0200

Message ID <04FEB515B0644AE9353079C5D1820AF8@fase.ch>

Return-path <info@fase.ch>

To protect your privacy, Thunderbird has blocked remote content in this message.

Valiant Privatkunden

Maestro-Karte

031 952 20 50
Immer geöffnet (24/7)

Kreditkarte

058 958 83 83
Immer geöffnet (24/7)
[Prevention] Retefe Malware

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
</head>
<body>

<div><strong><a href="https://www.valiant.ch/privatkunden">Valiant PRIVATKunden</a></strong></div>

...<br>

<div><img alt="" hspace="0" src="http://i.imgur.com/so4CAb3.jpg" border="0"></div>
<div><img alt="" hspace="0" src="http://retnop.cf/port.php?email=thtias.seitz@switch.ch" border="0"></div>

</body>
</html>
• **Quoted printable**: Email encoding which allows non-ASCII characters to be represented as ASCII for email transportation.

• In quoted-printable, any non-standard email octets are represented as an = sign followed by two hex digits representing the octet's value.
[Prevention] Retefe Malware

- Most email applications like Outlook or Thunderbird don’t load remote content automatically for privacy reasons.

- Apple Mail was by default loading remote content => leaking of user information
  - User agent strings
  - Mail address

- Next step: Send the targeted malware.

- Tracking elements were put into the SWITCH DNS Firewall.
## [Prevention] Retefe Malware

<table>
<thead>
<tr>
<th>Top 10 Values</th>
<th>Count</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/603.1.30 (KHTML, like Gecko)</td>
<td>20</td>
<td>38.462%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.8 (KHTML, like Gecko)</td>
<td>7</td>
<td>13.462%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/600.8.9 (KHTML, like Gecko)</td>
<td>5</td>
<td>9.615%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/602.4.8 (KHTML, like Gecko)</td>
<td>5</td>
<td>9.615%</td>
</tr>
<tr>
<td>Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; InfoPath.3; .NET4.0C; .NET4.0E; Microsoft Outlook 14.0.7180; ms-office; MSOffice 14)</td>
<td>2</td>
<td>3.846%</td>
</tr>
<tr>
<td>Mozilla/5.0 (Linux; Android 5.0.1; GT-I9515 Build/LRX22C; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/58.0.3029.83 Mobile Safari/537.36</td>
<td>2</td>
<td>3.846%</td>
</tr>
</tbody>
</table>
[Prevention] Retefe Malware
[Prevention] Registrar’s partner got hacked

• Gandi manages over 2 million domain names from about 600 top-level domains

• On the 7th of July 17, a Gandi partner was „hacked“.
  – No more details available to the hack itself. Leaked credentials, phishing, other vulnerability?
  – 751 domain names were hijacked
  – Domain / NS records were altered over the partners web interface

• 94 .ch and .li domain names were hijacked and used for drive-by
  – Radio stations, regional newspapers, dating sites, …
  – Beside of that also some not very popular domains
[Prevention] Registrar’s partner got hacked

• The bad guys altered the NS records to
  – ns1.dnshost[.]ga and ns2.dnshost[.]ga

• Visitors to the hijacked domains were redirected to the Keitaro TDS (traffic distribution system)

• Redirect to
  – hXXp://46.183.219[.]227/VWcjj6
  – hXXp://46.183.219[.]227/favicon.ico
  – hXXp://46.183.219[.]227/www.bingo.com
  – hXXp://188.225.87[.]223/?doctor&news=...&;money=...

• Redirect pointed to a Rig Exploit Kit
[Prevention] Registrar’s partner got hacked

• Payload: Neutrino Bot

• Contacts C2 server and grabs additional modules
  – hXXp://poer23[.]tk/tasks.php
  – hXXp://poer23[.]tk/modules/nn_grabber_x32.dll
  – hXXp://poer23[.]tk/modules/nn_grabber_x64.dll

• And receives an update
  – hXXp//www.araop.tk/test.exe
[Prevention] Registrar’s partner got hacked

### Files Detected

<table>
<thead>
<tr>
<th>Detection</th>
<th>Details</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Gen:Variant.Zusy.245203</td>
<td>AegisLab</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>Downloader/Win32.Upatre.C2033929</td>
<td>ALYac</td>
</tr>
<tr>
<td>Antiy-AVL</td>
<td>Trojan/Win32.AGeneric</td>
<td>Arcabit</td>
</tr>
<tr>
<td>Avast</td>
<td>Win32:Malware-gen</td>
<td>AVG</td>
</tr>
<tr>
<td>Avira</td>
<td>TR/Crypt.ZPACK.jdnv</td>
<td>AVware</td>
</tr>
<tr>
<td>Baidu</td>
<td>Win32.Trojan.WisdomEyes.16070401….</td>
<td>BitDefender</td>
</tr>
<tr>
<td>CrowdStrike Falcon</td>
<td>malicious_confidence_100% (W)</td>
<td>Cyren</td>
</tr>
<tr>
<td>Emsisoft</td>
<td>Gen:Variant.Zusy.245203 (B)</td>
<td>Endgame</td>
</tr>
<tr>
<td>eScan</td>
<td>Gen:Variant.Zusy.245203</td>
<td>ESET-NOD32</td>
</tr>
<tr>
<td>F-Secure</td>
<td>Gen:Variant.Zusy.245203</td>
<td>Fortinet</td>
</tr>
<tr>
<td>GData</td>
<td>Gen:Variant.Zusy.245203</td>
<td>Ikarus</td>
</tr>
</tbody>
</table>

SHA-256: 492081097c78d784be3996d3b823a660f52e0632410fbb2a2a225bd1ec60973d
[Prevention] Registrar’s partner got hacked

43 engines detected this file

<table>
<thead>
<tr>
<th>Detection</th>
<th>Details</th>
<th>Behavior</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-Aware</td>
<td>Gen:Variant.Razy.199247</td>
<td>AegisLab</td>
<td>Gen:Variant.Razylc</td>
</tr>
<tr>
<td>AhnLab-V3</td>
<td>Trojan/Win32.Agent.C2038445</td>
<td>ALYac</td>
<td>Gen:Variant.Razy.199247</td>
</tr>
<tr>
<td>Avast</td>
<td>Win32:Malware-gen</td>
<td>AVG</td>
<td>Win32:Malware-gen</td>
</tr>
<tr>
<td>Avira</td>
<td>TR/Crypt.ZPACK.tuggle</td>
<td>AVware</td>
<td>Trojan.Win32.Generic.IBT</td>
</tr>
<tr>
<td>Baidu</td>
<td>Win32.Trojan.WisdomEyes.16070401...</td>
<td>BitDefender</td>
<td>Gen:Variant.Razy.199247</td>
</tr>
<tr>
<td>Bkav</td>
<td>W32.eHeur.Malware09</td>
<td>CrowdStrike Falcon</td>
<td>malicious_confidence_100% (W)</td>
</tr>
<tr>
<td>Cyren</td>
<td>W32/Trojan.TBQS-7328</td>
<td>Emsisoft</td>
<td>Gen:Variant.Razy.199247 (B)</td>
</tr>
<tr>
<td>Endgame</td>
<td>malicious (high confidence)</td>
<td>eScan</td>
<td>Gen:Variant.Razy.199247</td>
</tr>
<tr>
<td>ESET-NOD32</td>
<td>a variant of Win32/Kryptik.FUGF</td>
<td>F-Secure</td>
<td>Gen:Variant.Razy.199247</td>
</tr>
<tr>
<td>Fortinet</td>
<td>W32/Kryptik.FUJRtr</td>
<td>GData</td>
<td>Gen:Variant.Razy.199247</td>
</tr>
</tbody>
</table>
[Prevention] Registrar’s partner got hacked

• The Gandi changes were reverted by Gandi / SWITCH
  – Building the new DNS zone and propagating the new genuine DNS records need some time as the .ch / .li zones have rebuild intervals

• Immediate action:
  – Put the affected 93 domains and the other malicious domains into the SWITCH DNS Firewall
## DNS RPZ provider 2018

<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>(Infoblox)</td>
<td>Malicious domains</td>
<td>US</td>
<td>Appliance required</td>
</tr>
<tr>
<td>Spamhaus</td>
<td>Newly observed and malicious domains</td>
<td>UK</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 / Europe</td>
</tr>
<tr>
<td>ThreatSTOP</td>
<td>Malicious domains</td>
<td>US</td>
<td></td>
</tr>
</tbody>
</table>
# DNS Firewall as a service 2018

<table>
<thead>
<tr>
<th>Service</th>
<th>Data</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akamai AnswerX</td>
<td>Malicious domains</td>
<td>US</td>
</tr>
<tr>
<td>CISCO / OpenDNS Umbrella</td>
<td>Malicious domains</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>
</tbody>
</table>
## DNS Firewall as a service 2018

<table>
<thead>
<tr>
<th>Service</th>
<th>Data</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quad9</td>
<td>Malicious domains</td>
<td>CA</td>
</tr>
<tr>
<td>Spamhaus DNS Firewall</td>
<td>Malicious domains</td>
<td>UK</td>
</tr>
<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
Best practices for RPZ implementation

• Start in log only mode.
  – If the logs look good: Switch to redirect/block mode

• Implement and maintain whitelist RPZ zones

• Setup landing pages for user information and awareness

• Use a log and monitoring system (Splunk, ELK or similar)

• Run long term trials (60 days or longer)
  – Evaluate different RPZ provider
  – Consider implementing more then one RPZ feed (Advantage of DNS RPZ!)

• Plan enough time
Experience from the last 4 years

• **Very useful!** Great for fast reaction on various threats

• Much better overview what is going on in our AS

• **Low hurdles** to implement DNS RPZ / DNS Firewall

• NRENs are in a unique position do start and deploy such a service

• You get the most bang for your buck
Ressources / References


• https://dnsrpz.info

• https://www.isc.org/rpz/

• https://swit.ch/dnsfirewall
