FCT Fundação para a Ciência e a Tecnologia

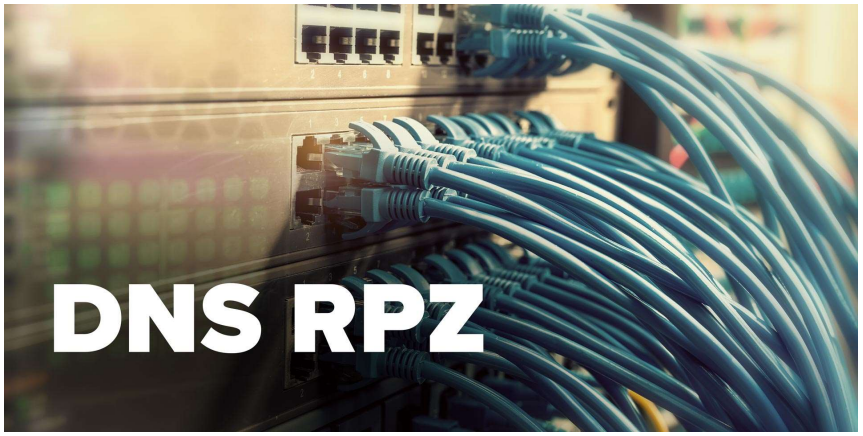
Computação Científica Nacional
FCCN

DNS Firewall @RCTS

Hélder Fernandes
ASA / SEG
20-Nov-2018

DNS-RPZ:O que é?

- **D**omain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones
- A.k.a. «DNS firewall»



DNS-RPZ:O que é?

- Mecanismo utilizado apenas por DNS resolvers
- Permite modificar as respostas na resolução de DNS de um ou mais domínios
- Eficaz quando se pretende impedir o acesso a domínios não desejados (DNS Sinkhole)

DNS-RPZ @RCTS: Implementação na RCTS

- Em piloto desde Fev/2017

- A bloquear acessos desde DEZ/2017

- Atualmente 10 instituições da RCTS a usar este serviço

Universidade do Minho

LNEG

LABORATÓRIO NACIONAL DE ENGENHARIA CIVIL

ipb INSTITUTO POLITÉCNICO DE BRAGANÇA

ipt Instituto Politécnico de Tomar

utad UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

Instituto Politécnico de Castelo Branco

U.PORTO

POLITÉCNICO DE LISBOA

IPCA INSTITUTO POLITÉCNICO DO CÁVADO E DO AVE

Serviços DNS-RPZ no Mercado

LAYER8

DNS8

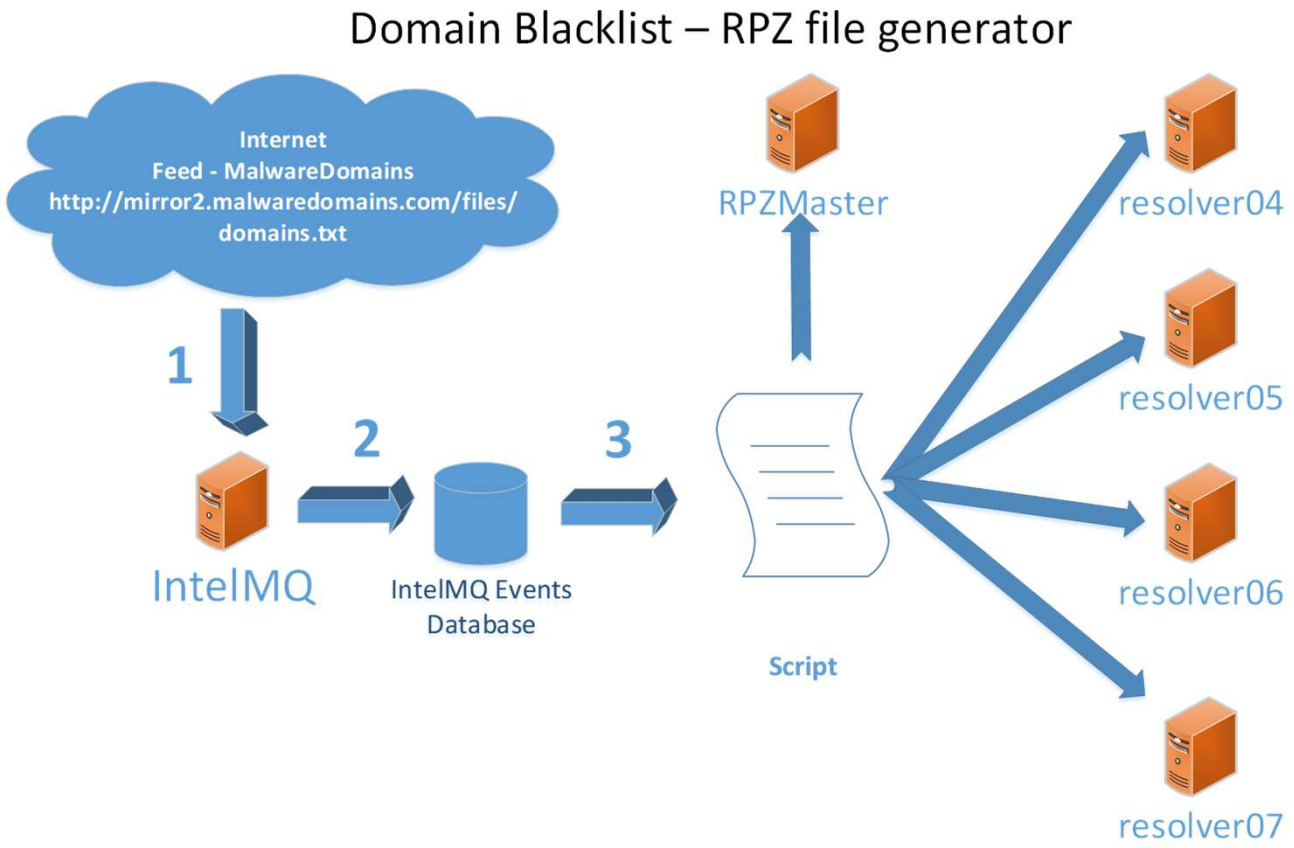
CLOUDFLARE

BLUECAT

cisco Cisco Umbrella

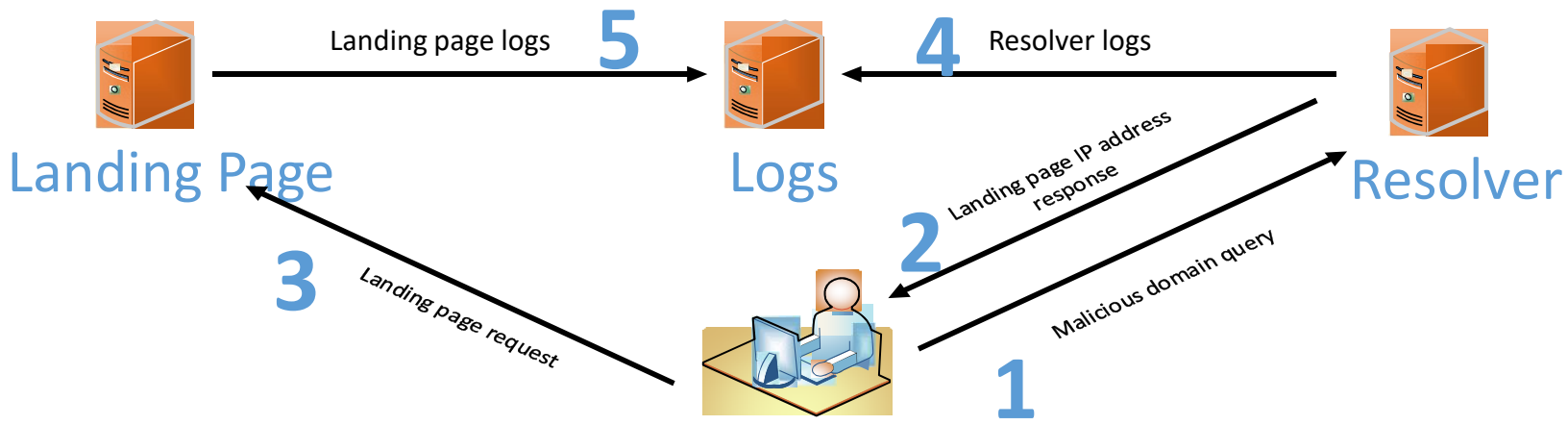
efficient iP™
DEFINING SMART DDI

Criação de Zonas para o RPZ

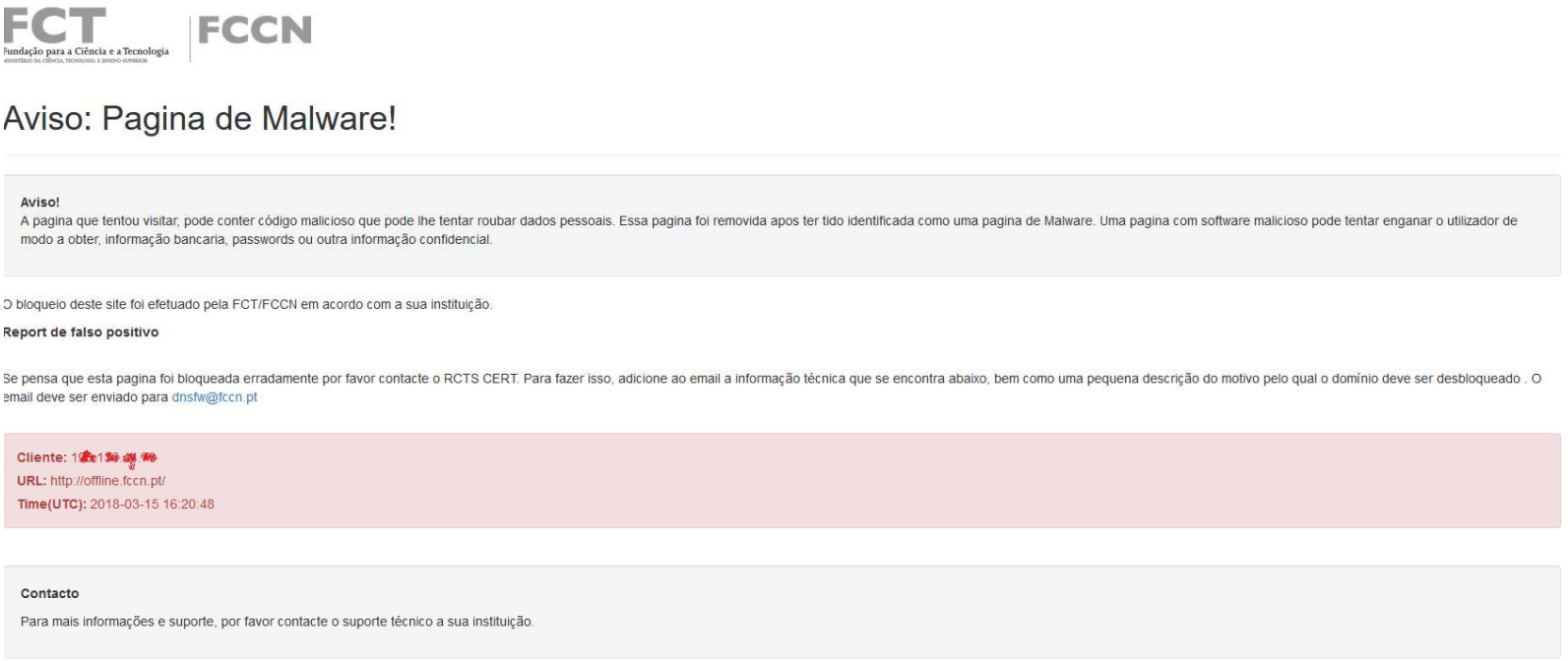


DNS-RPZ @ RCTS – Landing Page

- Implementação de uma *"Landing page"*
- Interativo em tráfego http/https
- Recolha de dados na Landing page para análise



DNS-RPZ @ RCTS – Landing Page



DNS-RPZ na RCTS – Landing Page

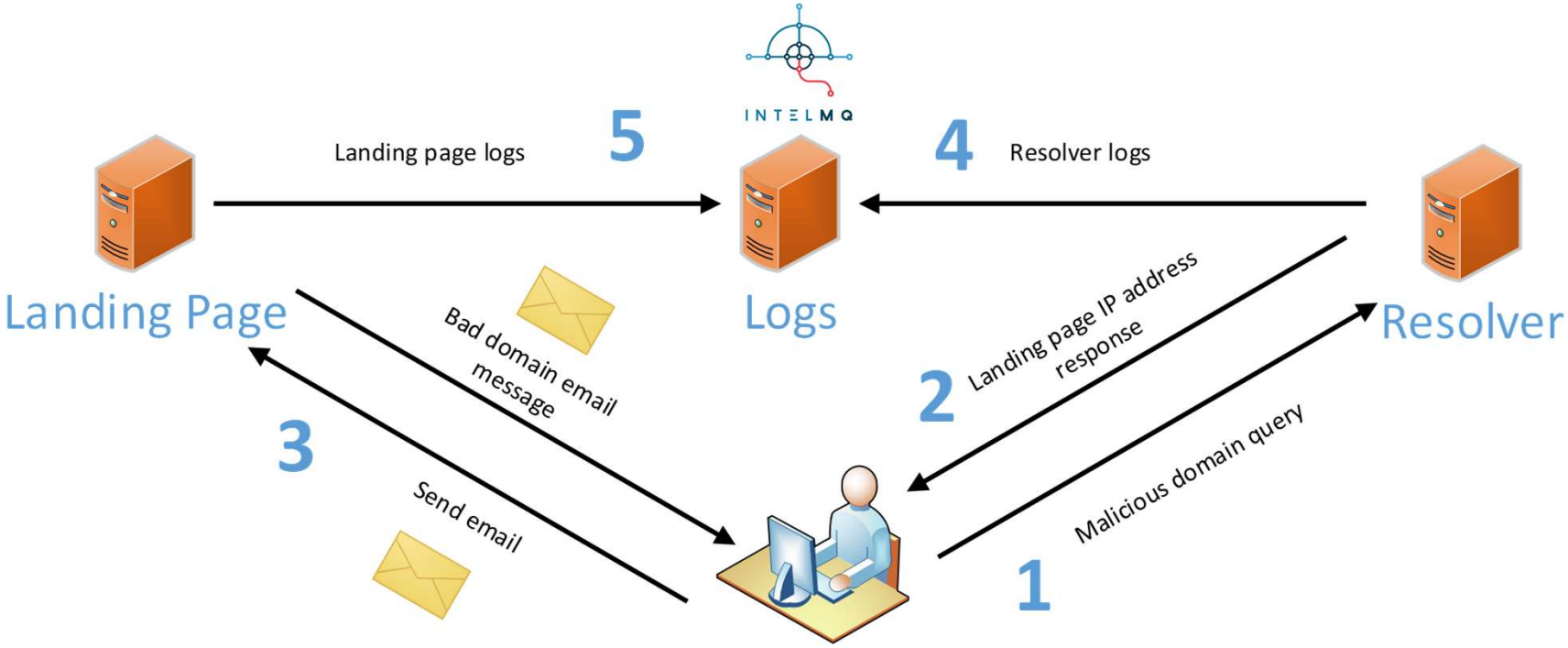
- Recolha de dados do pedido do cliente


```
{ [-]
   accesstype: url
   client_ip: [redacted]
   date_time: 2018-02-06 09:49:58 UTC
   domain: coinhive.com
   domain_type: maliciousjs
   from:
   http_method: GET
   observation_time: 2018-02-06T09:50:01
   post_data:
   rcpt:
   url: https://coinhive.com/lib/coinhive.min.js
   user_agent: Mozilla/5.0 (Linux; Android 5.1; ROME_X Build/LMY47I) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/39.0.0.0 Mobile Safari/537.36
}
```

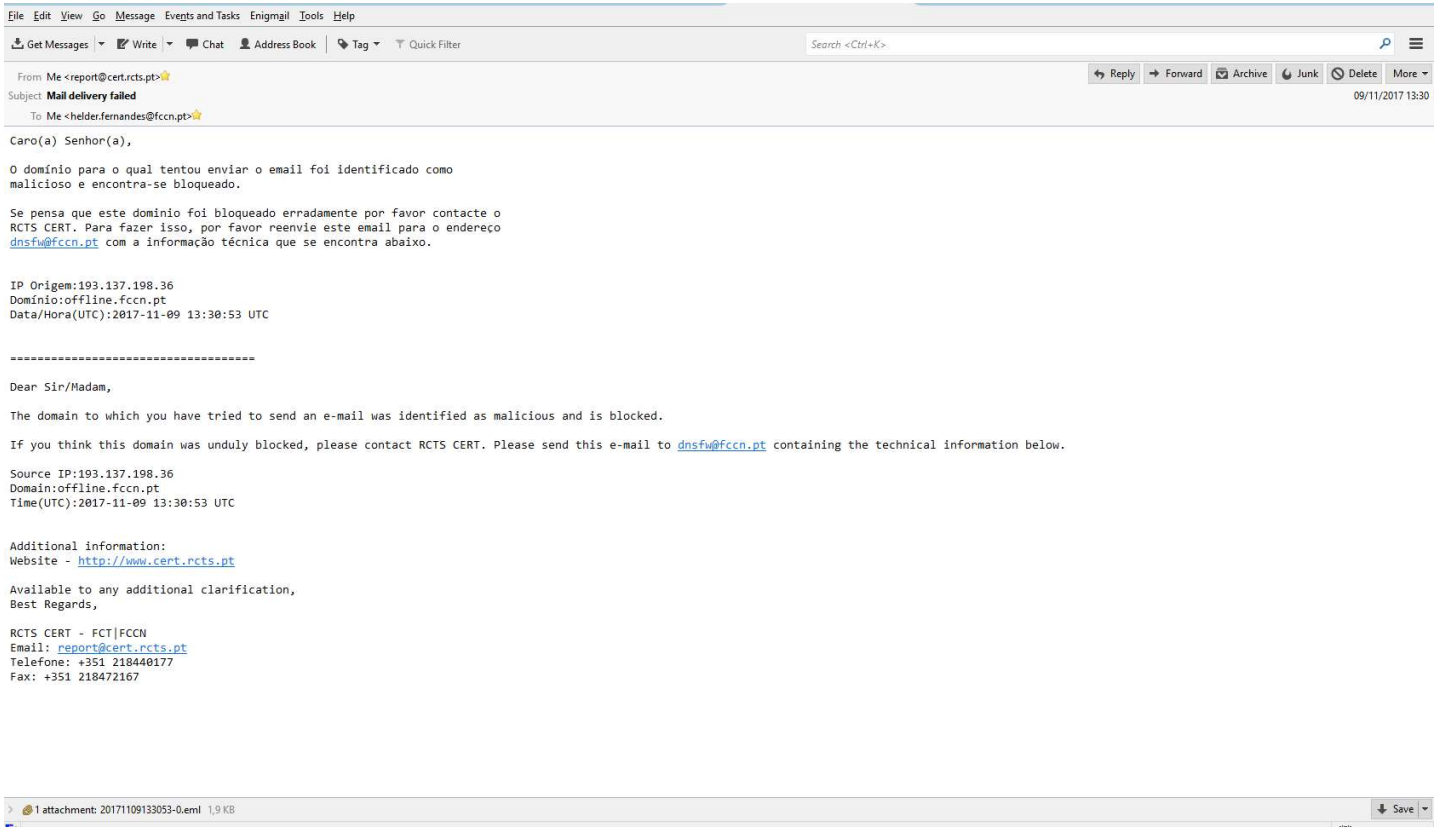
```
{ [-]
   accesstype: url
   client_ip: [redacted]
   date_time: 2018-03-15 23:52:45 UTC
   domain: gimnasiofitness.co
   domain_type: phishing
   from:
   http_method: POST
   observation_time: 2018-03-15T23:55:01
   post_data:
   rcpt:
   url: http://gimnasiofitness.co/wp-content/plugins/goodbarber/controllers/asbfqgqa.php
   user_agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_1 like Mac OS X) AppleWebKit/603.1.30 (KHTML,
like Gecko) Version/10.0 Mobile/14E304 Safari/602.1ke Gecko) Version/10.0 Mobile/14E304 Safari/602.1
}
```

DNS-RPZ @ RCTS – SMTP SINK

- Implementação de “*smtp sink*”



DNS-RPZ @ RCTS – SMTP SINK



File Edit View Go Message Events and Tasks Enigmail Tools Help

Get Messages | Write | Chat | Address Book | Tag | Quick Filter | Search <Ctrl+K>

Reply | Forward | Archive | Junk | Delete | More

From Me <report@cert.rcts.pt>

Subject **Mail delivery failed** 09/11/2017 13:30

To Me <helder.fernandes@fccn.pt>

Caro(a) Senhor(a),

O domínio para o qual tentou enviar o email foi identificado como
malicioso e encontra-se bloqueado.

Se pensa que este dominio foi bloqueado erradamente por favor contacte o
RCTS CERT. Para fazer isso, por favor reenvie este email para o endereço
dnsfw@fccn.pt com a informação técnica que se encontra abaixo.

IP Origem:193.137.198.36
Domínio:offline.fccn.pt
Data/Hora(UTC):2017-11-09 13:30:53 UTC

==========

Dear Sir/Madam,

The domain to which you have tried to send an e-mail was identified as malicious and is blocked.

If you think this domain was unduly blocked, please contact RCTS CERT. Please send this e-mail to dnsfw@fccn.pt containing the technical information below.

Source IP:193.137.198.36
Domain:offline.fccn.pt
Time(UTC):2017-11-09 13:30:53 UTC

Additional information:
Website - http://www.cert.rcts.pt

Available to any additional clarification,
Best Regards,

RCTS CERT - FCT|FCCN
Email: report@cert.rcts.pt
Telefone: +351 218440177
Fax: +351 218472167

1 attachment: 20171109133053-0.eml 1,9 KB | Save

DNS-RPZ @ RCTS – Gestão dos Feeds

- Várias fontes, não pagas
- Análise de Malware
  - IoCs adicionados pelo RCTS CERT
  - Utilização de ferramentas, como o Cuckoo
  - Aberto a IoCs de outros CSIRTs

DNS-RPZ @ RCTS – Gestão dos Feeds

Domain Blacklist 1.0

1 2 3 4 5 6 7 8 9 10 11 Next

Protect this directory with .htaccess

id ▾ Search Add Record

	id	Dominio	Tipo	Feed_url	Feed	Last_seen
	6260349	zahntechnik-imlau.de	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260348	topwebmaster.su	suspicious	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260347	sigmanet.gr	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260346	servicesseront.com	phishing	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260345	projex-dz.com	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260344	partlcle.com	suspicious	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260343	laghartruan.com	phishing	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260342	internet-webshops.de	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260341	hotelruota.it	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260340	hobbystube.net	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00
	6260339	hilaryandsavio.com	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00

DNS-RPZ @ RCTS – ZONAS

Existem atualmente 2 zonas a ser distribuídas:

- Zona com domínios DGA – 373161 domínios
- Zona principal – 27123 domínios

DNS-RPZ @ RCTS – IMPLEMENTAÇÃO

Existem atualmente 3 formas possíveis de implementar:

- Usando os servidores recursivos da FCT|FCCN
- Usando os servidores recursivos locais:
  - Transferência de zonas por AXFR
  - Transferência de zonas através scp

DNS-RPZ @ RCTS

Obrigado

Pedidos de adesão: **dnsfw@fccn.pt**

FCT Fundação para a Ciência e a Tecnologia

Computação Científica Nacional
FCCN

Obrigado pela atenção!

info@cert.rcts.pt