

**FCT**

Fundação para a Ciência e a Tecnologia  
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR

**FCCN**

Computação  
Científica Nacional

# DNS Firewall

Carlos Friaças



# Agenda

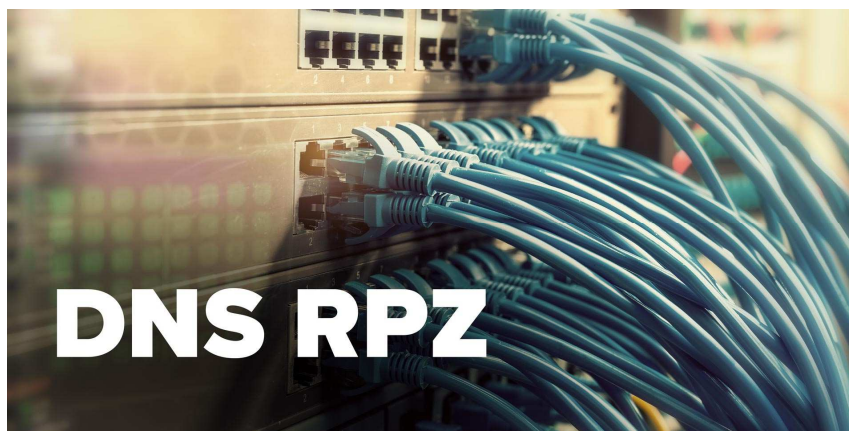
- DNS-RPZ
- RCTS DNS FIREWALL



# DNS RPZ

# DNS-RPZ:O que é?

- Domain Name Service Response Policy Zones
- 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)

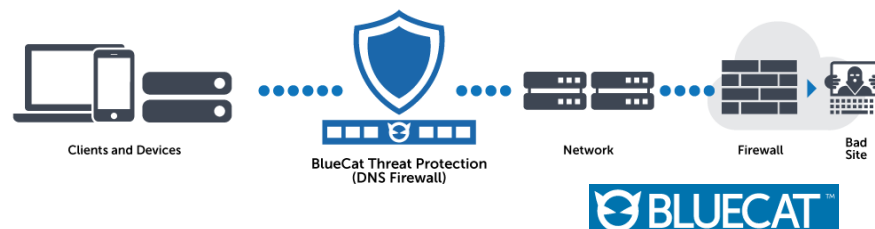




# Serviços DNS-RPZ no Mercado

LAYER8  
DNS8

  
CLOUDFLARE®



 Cisco Umbrella

 **efficient IP**<sup>TM</sup>  
DEFINING SMART DDI

# RCTS DNS FIREWALL

# RCTS DNS FIREWALL



## ***DNS Firewall***

O serviço ***DNS Firewall*** é um mecanismo que dificulta a infeção de sistemas por *malware*, através da alteração das respostas do protocolo *DNS*, quando é solicitada a resolução de nomes de domínios já identificados como maliciosos.

[www.fccn.pt](http://www.fccn.pt) Email: [info@cert.rcts.pt](mailto:info@cert.rcts.pt) Telefone: +351 21 8440177

### Malware

O *Malware* assume várias formas e é uma ameaça a todos os utilizadores da Internet. A divulgação do *malware* ocorre por diversos vetores, exigindo não só mais e melhores mecanismos empregues no seu combate, como sobretudo mais atenção e sensibilização para o problema por parte de todos os utilizadores.

### Áreas de intervenção

- Impedir infeções com base em conhecimento prévio sobre o carácter malicioso de diversos domínios;
- Auxílio na identificação de sistemas já infetados.

### Como funciona o serviço?

Este serviço é baseado no serviço de resolução de nomes, prestado no âmbito da RCTS. Cada membro da RCTS é livre de usar o seu próprio servidor de resolução de nomes, recorrer a um servidor externo, ou usar o serviço fornecido pela FCCN em [resolver.fccn.pt](http://resolver.fccn.pt). Quando surge um pedido de resolução sobre um domínio malicioso, é apresentada uma página de alerta, baseada na URL [offline.fccn.pt](http://offline.fccn.pt). A lista de domínios maliciosos é atualizada diariamente, sem intervenção humana, e com base em diversas fontes de informação. Todos os dias são identificados novos domínios.

### Como aderir

O *DNS Firewall* está disponível para todas as entidades ligadas à RCTS, não apresentando custos adicionais. A subscrição do serviço depende apenas do envio de um pedido para [info@cert.rcts.pt](mailto:info@cert.rcts.pt).



# RCTS DNS FIREWALL

- Em piloto desde Fev/2017
- A bloquear acessos desde Dez/2017
- DNS AXFR ou Secure Copy



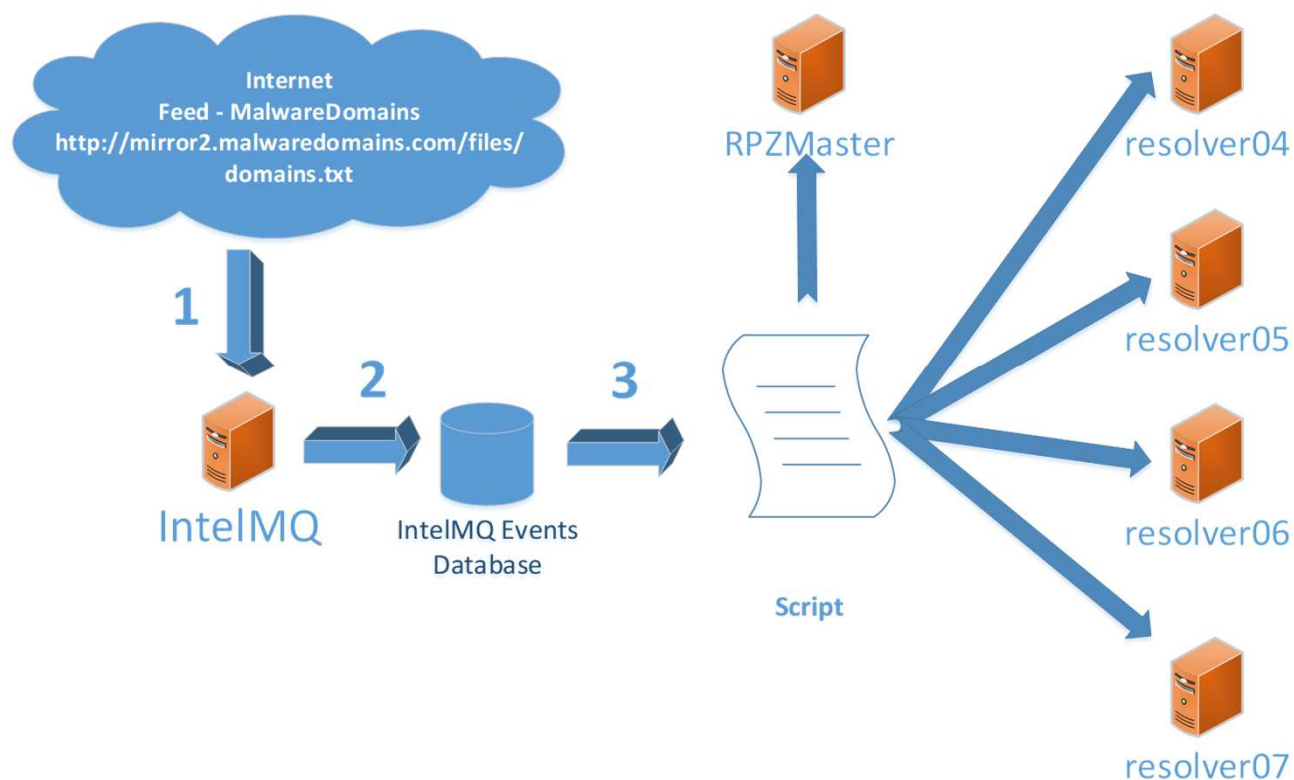
# RCTS DNS FIREWALL

- Atualmente 20 instituições da RCTS a usar este serviço
- Cerca de 2.500.000 domínios actualmente



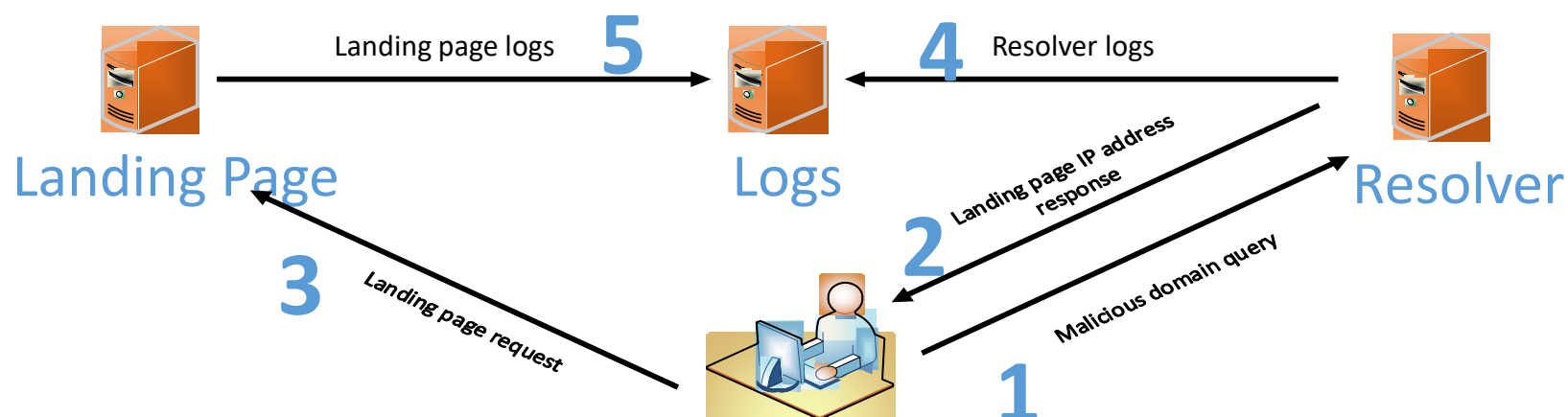
# Criação de Zonas

## Domain Blacklist – RPZ file generator



# Landing Page

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



# Landing Page

## Aviso: Pagina de Malware!

### Aviso!

A pagina que tentou visitar, pode conter código malicioso que pode lhe tentar roubar dados pessoais. Essa pagina foi removida apos ter sido identificada como uma pagina de Malware. Uma pagina com software malicioso pode tentar enganar o utilizador de modo a obter, informação bancaria, passwords ou outra informação confidencial.

O bloqueio deste site foi efetuado pela FCT/FCCN em acordo com a sua instituição.

### Report de falso positivo

Se pensa que esta pagina foi bloqueada erradamente por favor contacte o RCTS CERT. Para fazer isso, adicione ao email a informação técnica que se encontra abaixo, bem como uma pequena descrição do motivo pelo qual o domínio deve ser desbloqueado . O email deve ser enviado para [dnstfw@fccn.pt](mailto:dnstfw@fccn.pt)

Cliente: 10.10.10.10

URL: <http://offline.fccn.pt/>

Time(UTC): 2018-03-15 16:20:48

### Contacto

Para mais informações e suporte, por favor contacte o suporte técnico a sua instituição.



# Landing Page

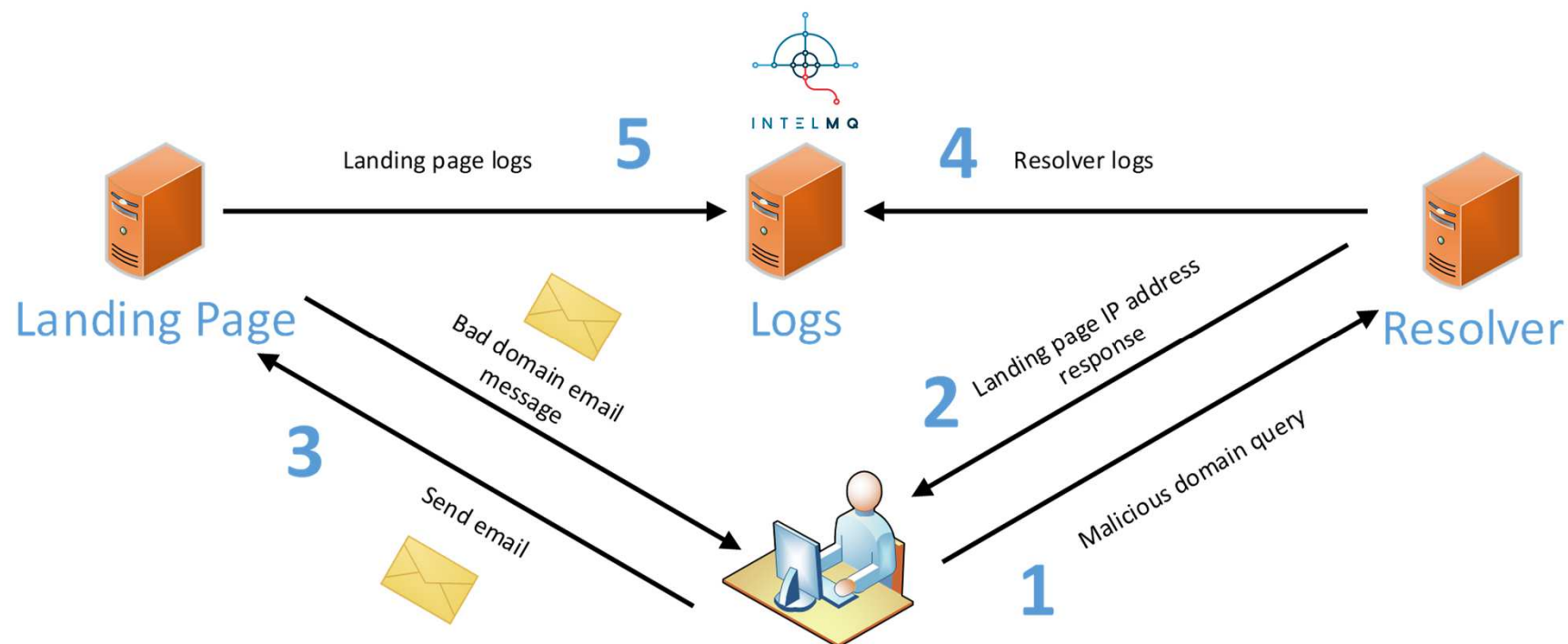
- Recolha de dados do pedido do cliente

```
{ [-]
  accesstype: url
  client_ip: 193.205.254.254
  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; ROMEX Build/LMY47I) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
  Chrome/39.0.0.0 Mobile Safari/537.36
}
```

```
{ [-]
  accesstype: url
  client_ip: 193.205.254.254
  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
}
```

# SMTP SINK

- Implementação de “*smtp sink*”



# 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>

From Me <report@cert.rcts.pt>★  
Subject Mail delivery failed  
To Me <helder.fernandes@fccn.pt>★

09/11/2017 13:30

Reply Forward Archive Junk Delete More

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 domínio foi bloqueado erradamente por favor contacte o RCTS CERT. Para fazer isso, por favor reenvie este email para o endereço [dnswfw@fccn.pt](mailto:dnswfw@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 [dnswfw@fccn.pt](mailto:dnswfw@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](mailto:report@cert.rcts.pt)  
Telephone: +351 218440177  
Fax: +351 218472167

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

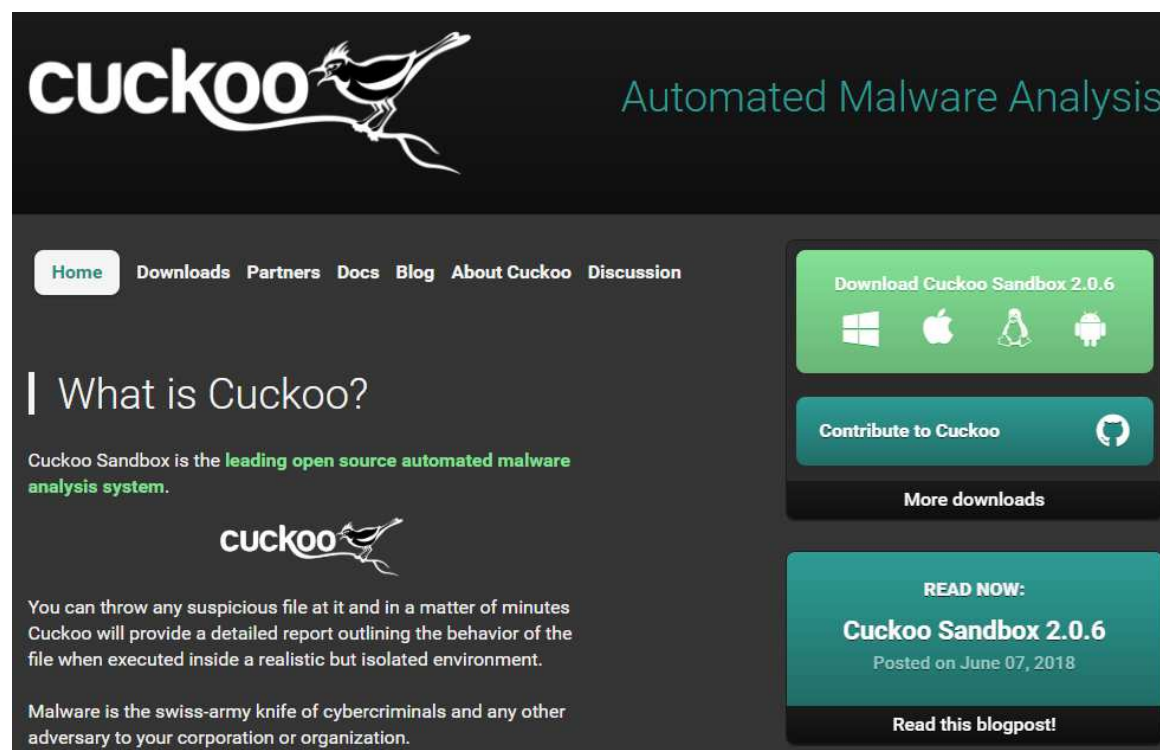
# Gestão dos Feeds

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



# Cuckoo

- <https://cuckoosandbox.org>
















# 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-implau.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	particle.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	hilarityandsavio.com	malware	spamhaus.org	malwaredomains	2017-10-31 00:00:00	

# Zonas

Existem atualmente duas zonas a ser distribuídas:

- Zona principal
- Zona com domínios DGA



# 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



# Em Resumo



DNS-RPZ é um mecanismo de combate ao malware



Queries DNS maliciosas desviadas para uma «Landing Page»



Todos podem contribuir para manter a lista de domínios maliciosos



# Obrigado