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

FCCN
Computação Científica Nacional

DNS-RPZ @RCTS

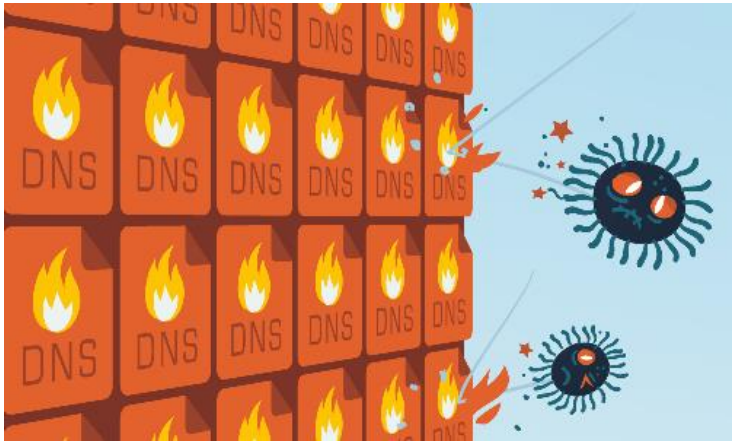
CERT RCTS

Carlos Friaças
Novembro 2017

DNS-RPZ: O que é?

- **D**omain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones

- A.k.a. «DNS firewall»

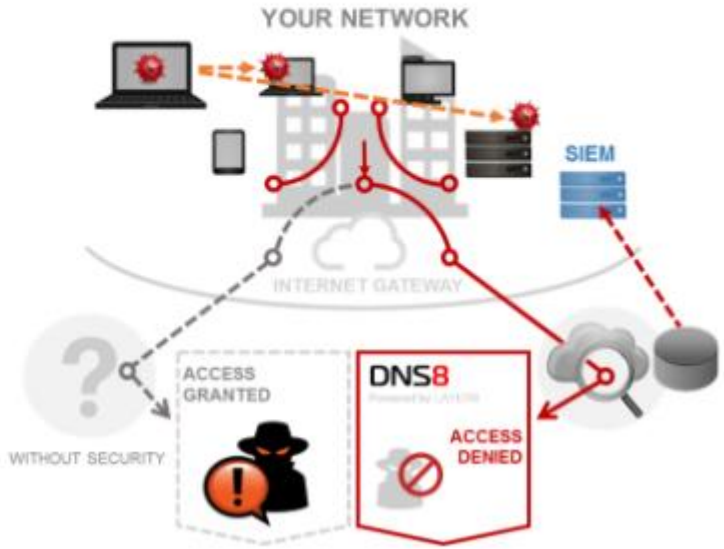


(Ilustração por Christoph Frei)

DNS-RPZ no Mercado, PT

DNS8

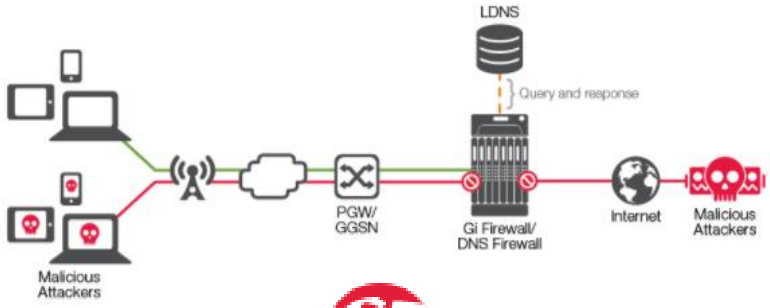
A service based on DNS (Domain Name System) service for malware and malicious websites access prevention. Using DNS Response Policy Zones (RPZs) it's possible to define policies that minimize impact from virus, Trojans, ransomware and other malware in enterprise networks.



DNS-RPZ no mercado

CLOUDFLARE

Shield Your DNS Infrastructure From DDoS Attacks With Cloudflare's DNS Firewall



efficient iP™
DEFINING SMART DDI

DNS Firewall

Protect Users and Block DNS-Based Malware Activity

cisco Cisco Umbrella

BLUECAT™

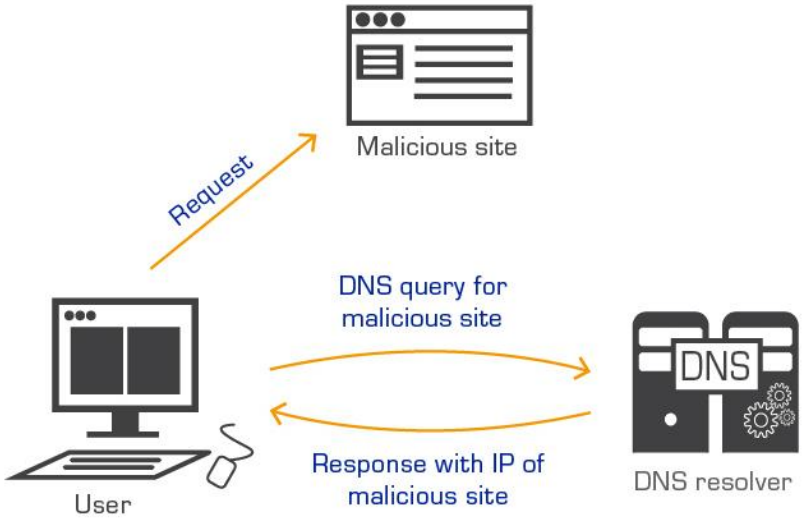
DNS-RPZ em NRENs: SWITCH

SWITCH

SWITCHcert | About us | Services | Info-Desk | SWITCH-CERT Report | Contact / RFC 2350

SWITCH DNS Firewall

The SWITCH DNS Firewall service reduces IT operating risks by preventing infections and identifying systems that are already infected, all with a minimum of effort. This service protects all company devices, such as laptops, servers and mobile phones, that use the company's DNS service.



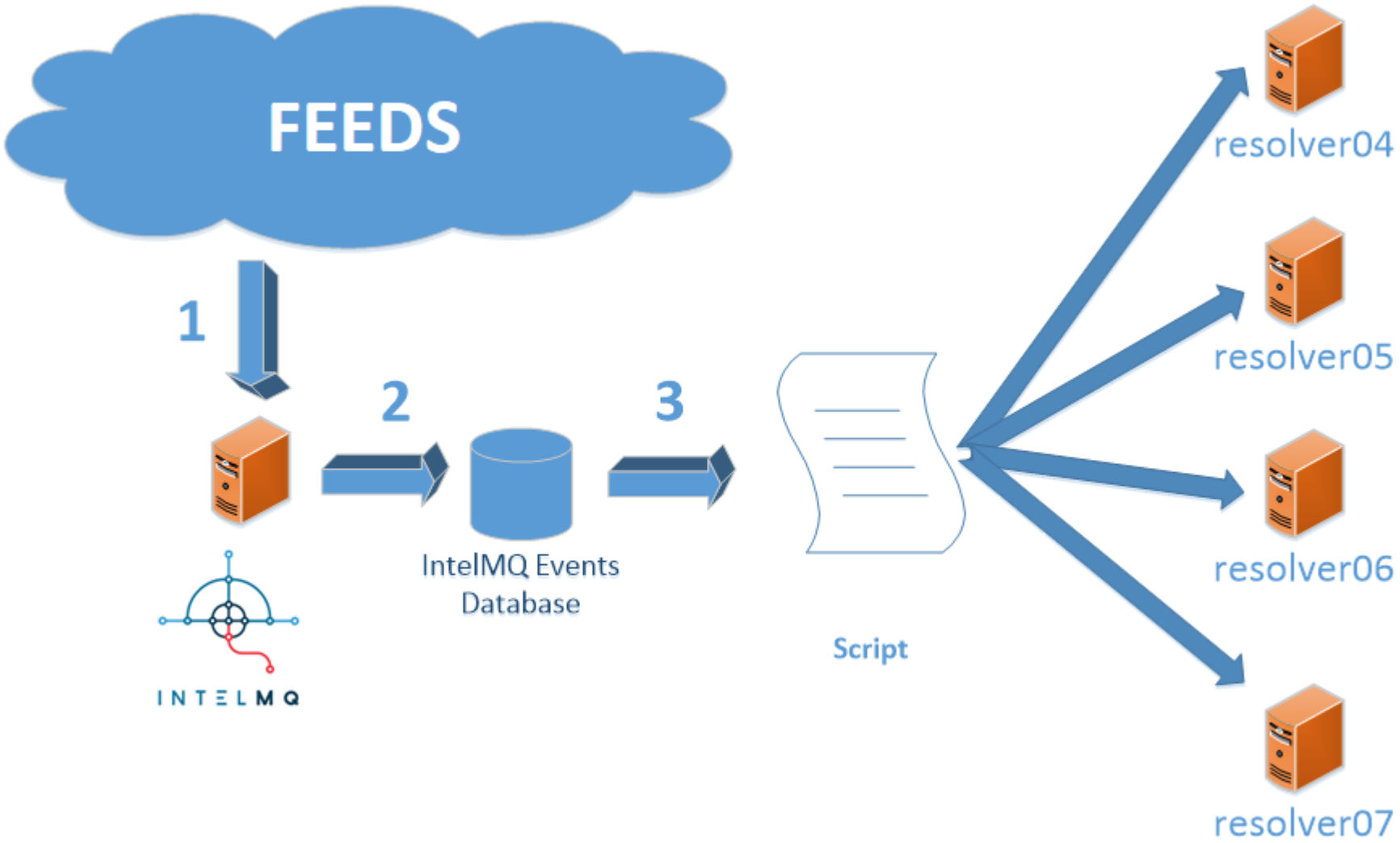
DNS-RPZ: Objectivos

- Auxiliar no combate a:
  - Phishing
  - Malware
  - Exploits
  - Código malicioso
  - Ransomware

DNS-RPZ: Objectivos

- Impedir a resolução DNS de domínios «maliciosos»
  - wgwuhauaqcrx.com
  - wpqjbffo.ru
  - tescobank.customerservice.atidecor.com
- Centenas de novos domínios maliciosos por dia

DNS-RPZ: Arquitectura @RCTS



DNS-RPZ @RCTS: Como?

- Em piloto desde Fev/2017
- Apenas está a fazer *«log»*
  - Não está ainda a rejeitar *queries*
- Activação: 4 de Dezembro
  - i.e. Iniciar rejeição de *queries*

DNS-RPZ @RCTS: Como?

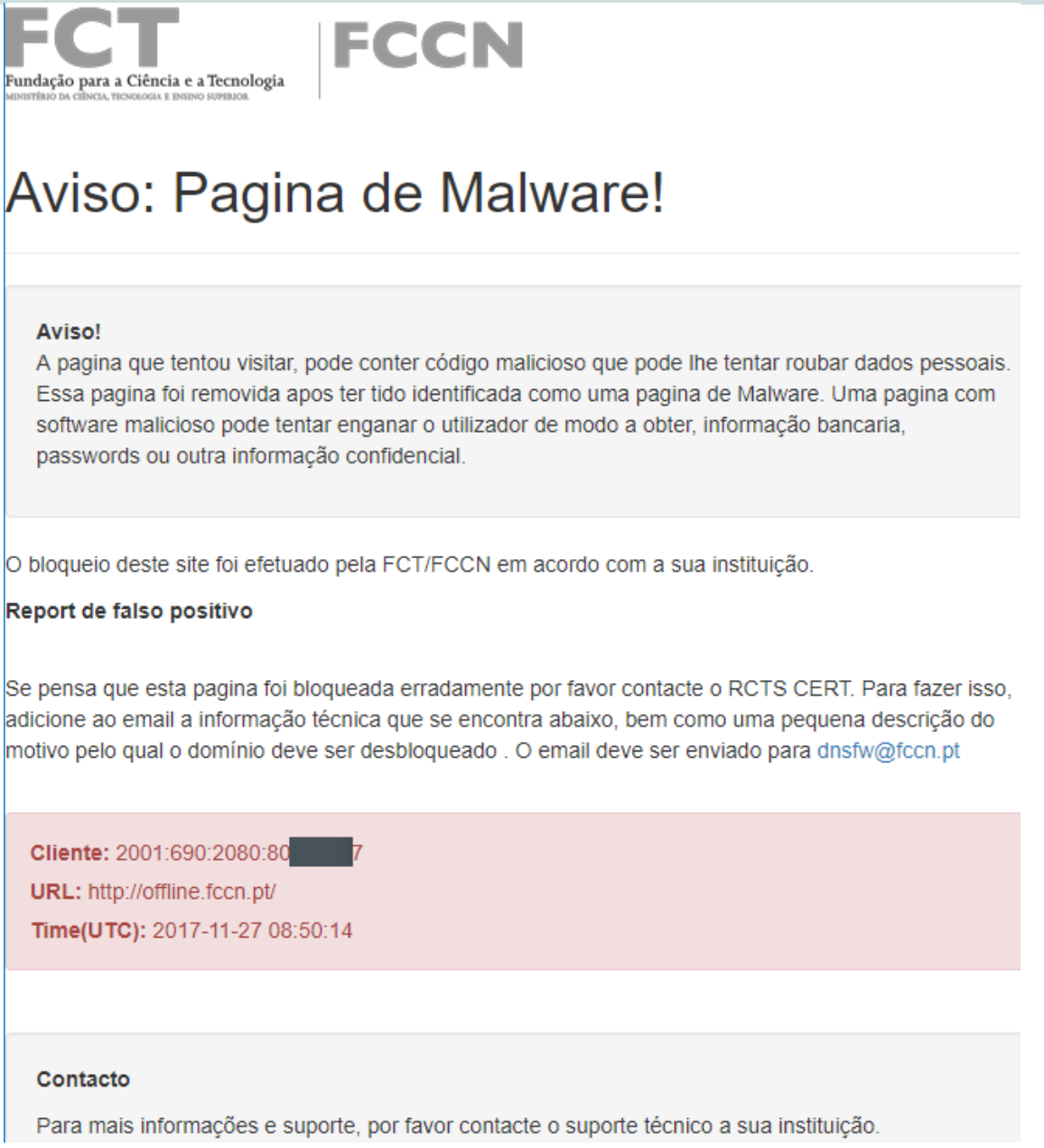
- Opção I: resolver.fccn.pt
  - 193.136.192.45
  - 2001:690:a00:4001::100

- Opção II: Fornecimento da zona para instalação em resolvers de instituições

DNS-RPZ @RCTS: Opção I

- «OPT-IN»
- A pedido de cada membro da RCTS
  - dnsfw@fccn.pt
- As redes IP da instituição (origem dos pedidos DNS) serão adicionadas à configuração
  - Para os restantes membros as respostas do resolver.fccn.pt não são afectadas

DNS-RPZ @RCTS: Opção I, «Landing Page»



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

FCCN

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 tido 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 dnsfw@fccn.pt

Cliente: 2001:690:2080:80[redacted]7
URL: http://offline.fccn.pt/
Time(UTC): 2017-11-27 08:50:14

Contacto

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

DNS-RPZ @RCTS: Opção II

- Pedido indicando endereço IP que obterá a informação
  - dnsfw@fccn.pt
  - Será adicionado a uma «whitelist»

DNS-RPZ @RCTS: 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: 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: FALSOS POSITIVOS

- O interface permite excluir domínios, de forma manual, se necessário

- É importante comunicar os falsos positivos encontrados
  - dnsfw@fccn.pt
  - Permitirá a melhoria do serviço

Obrigado