PORTUGAL INCoDe.2030

DNS-RPZ @RCTS

3ª Reunião da Rede Académica de CSIRT

Hélder Fernandes

helder.fernandes@fccn.pt

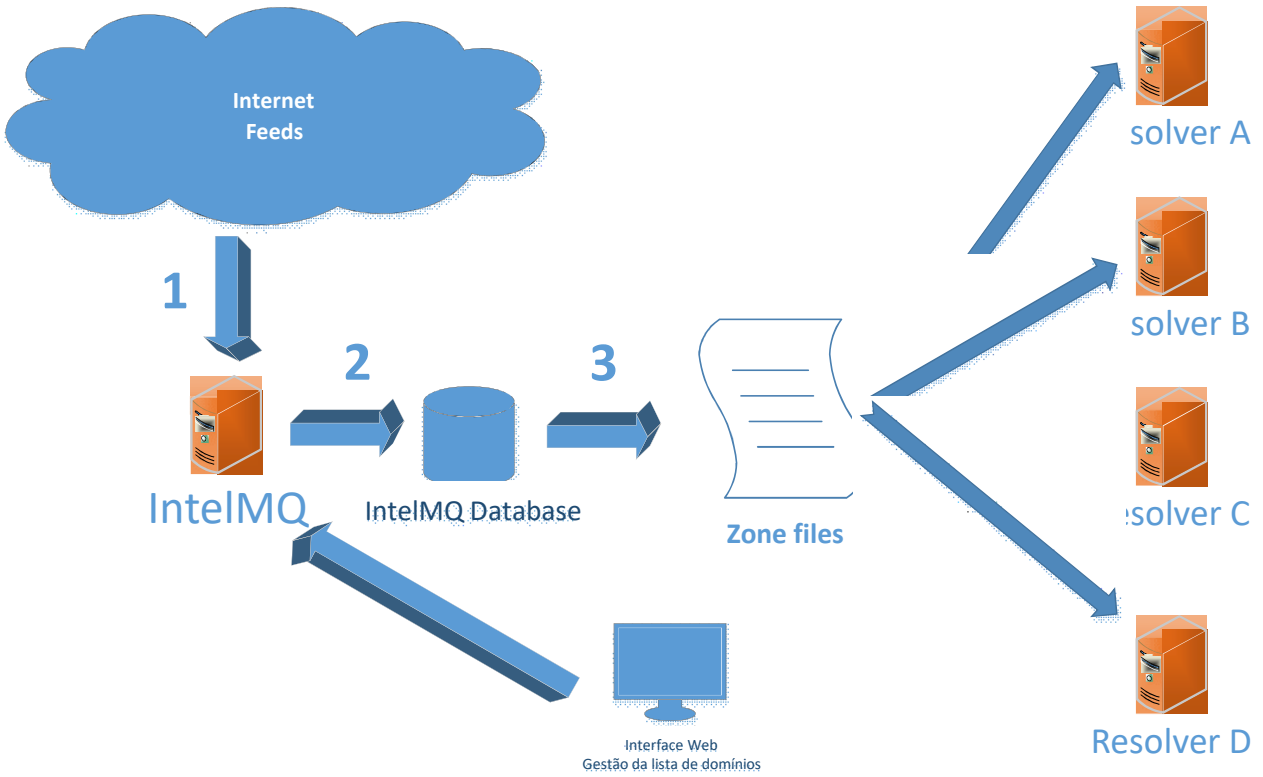
2018-04-13

DNS-RPZ: O que é?

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

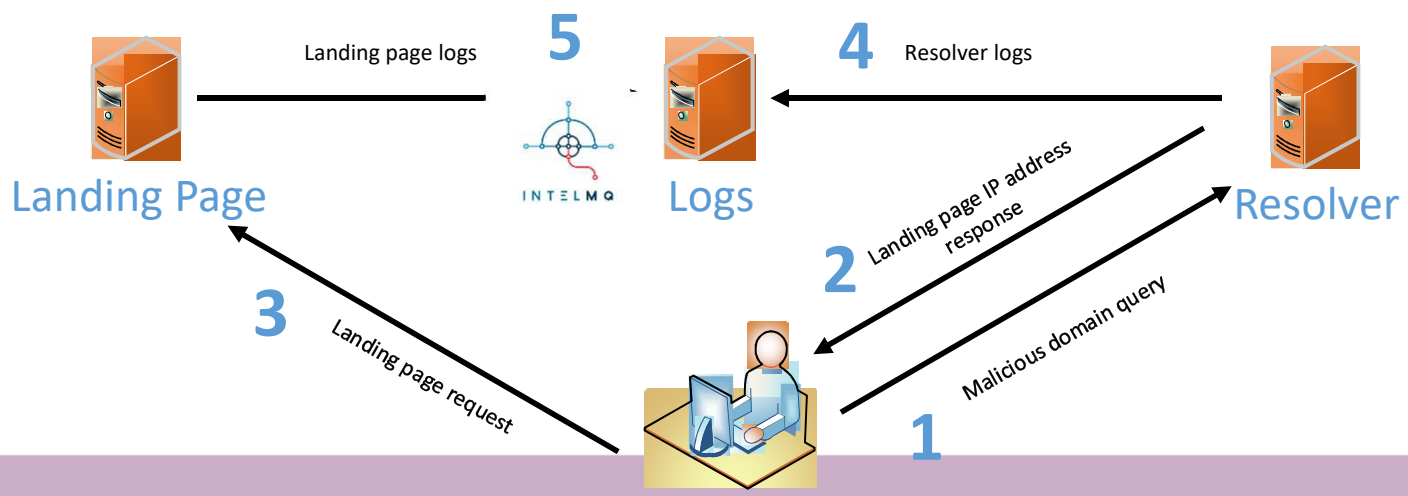
(Ilustração por Christoph Frei)

Arquitetura



Landing Page

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

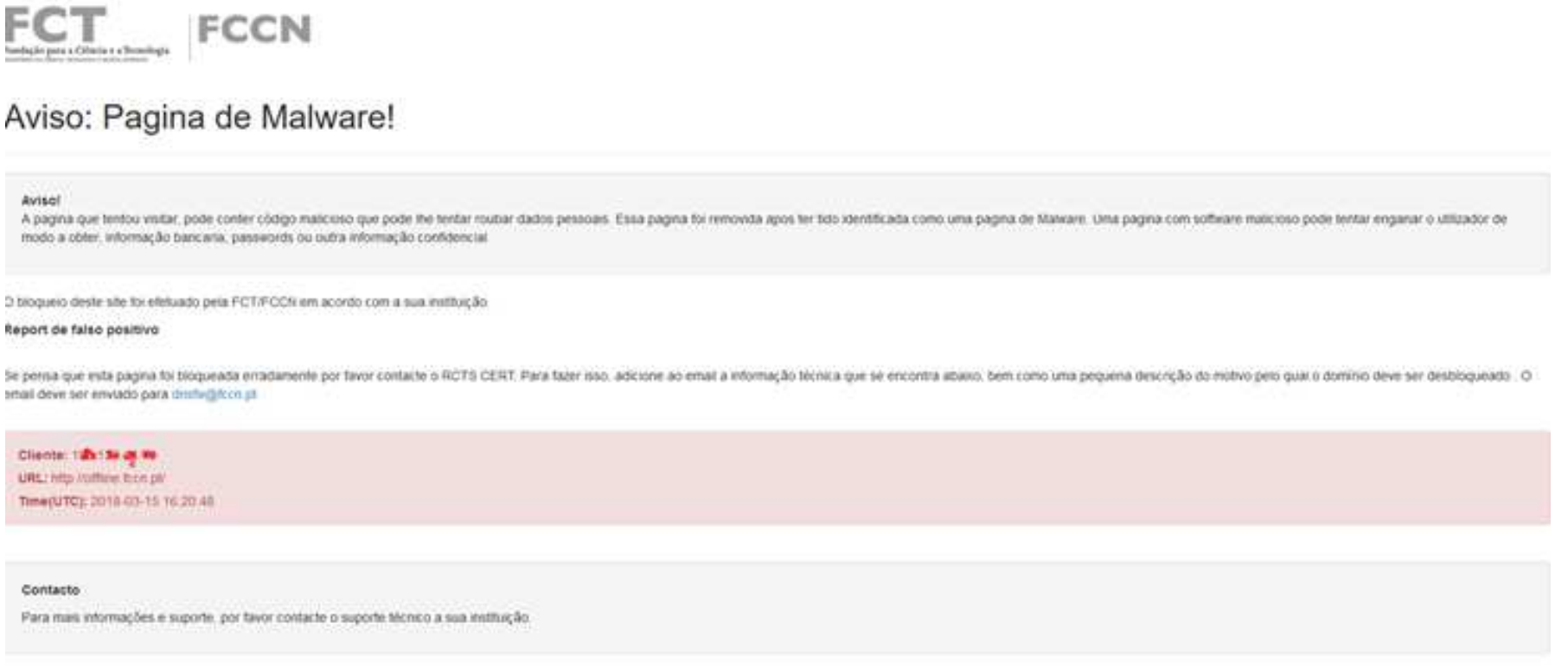


Recolha de dados do pedido do cliente

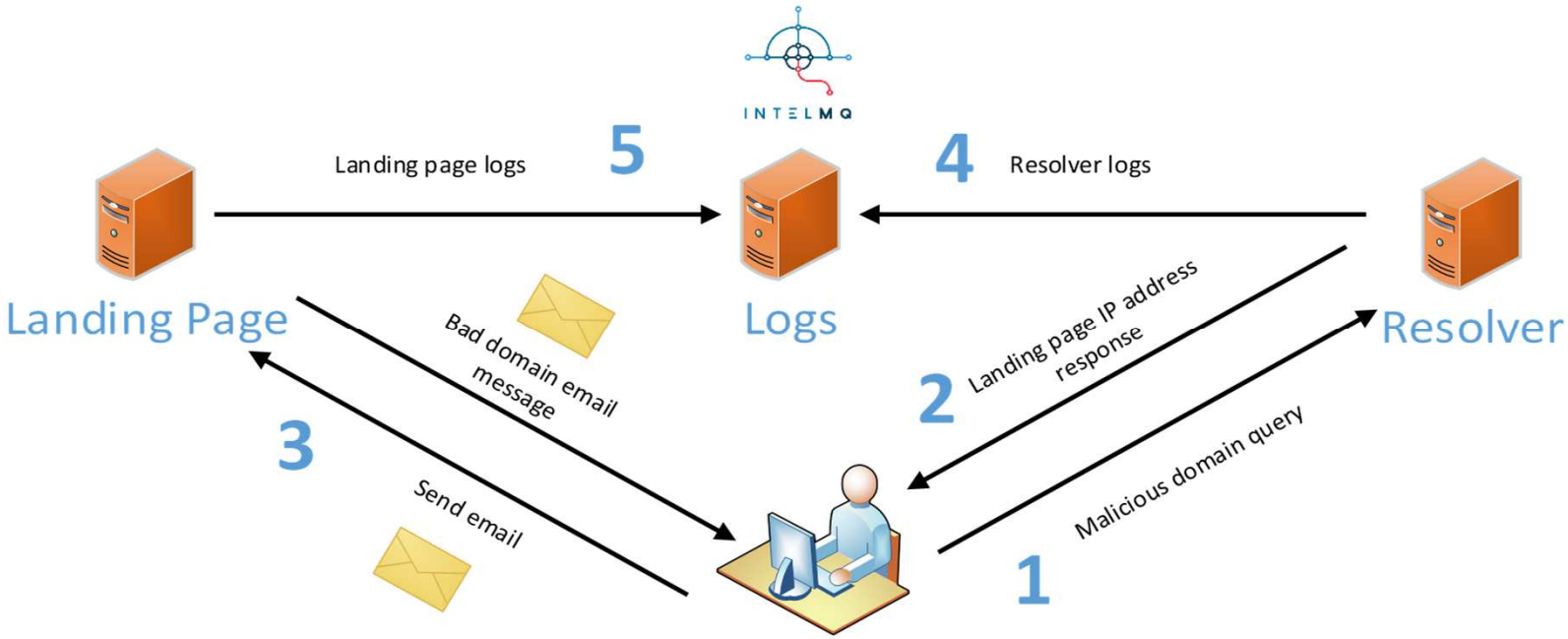

```
{ [-]
   accesstype: url
   client_ip: [redacted]
   date_time: 2018-02-06 09:49:58 UTC
   domain: coinhive.com
   domain_type: maliciousjs
   from:
   http_method: GET
   observation_time: 2018-02-06T09:50:01
   post_data:
   rcpt:
   url: https://coinhive.com/lib/coinhive.min.js
   user_agent: 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
}
```

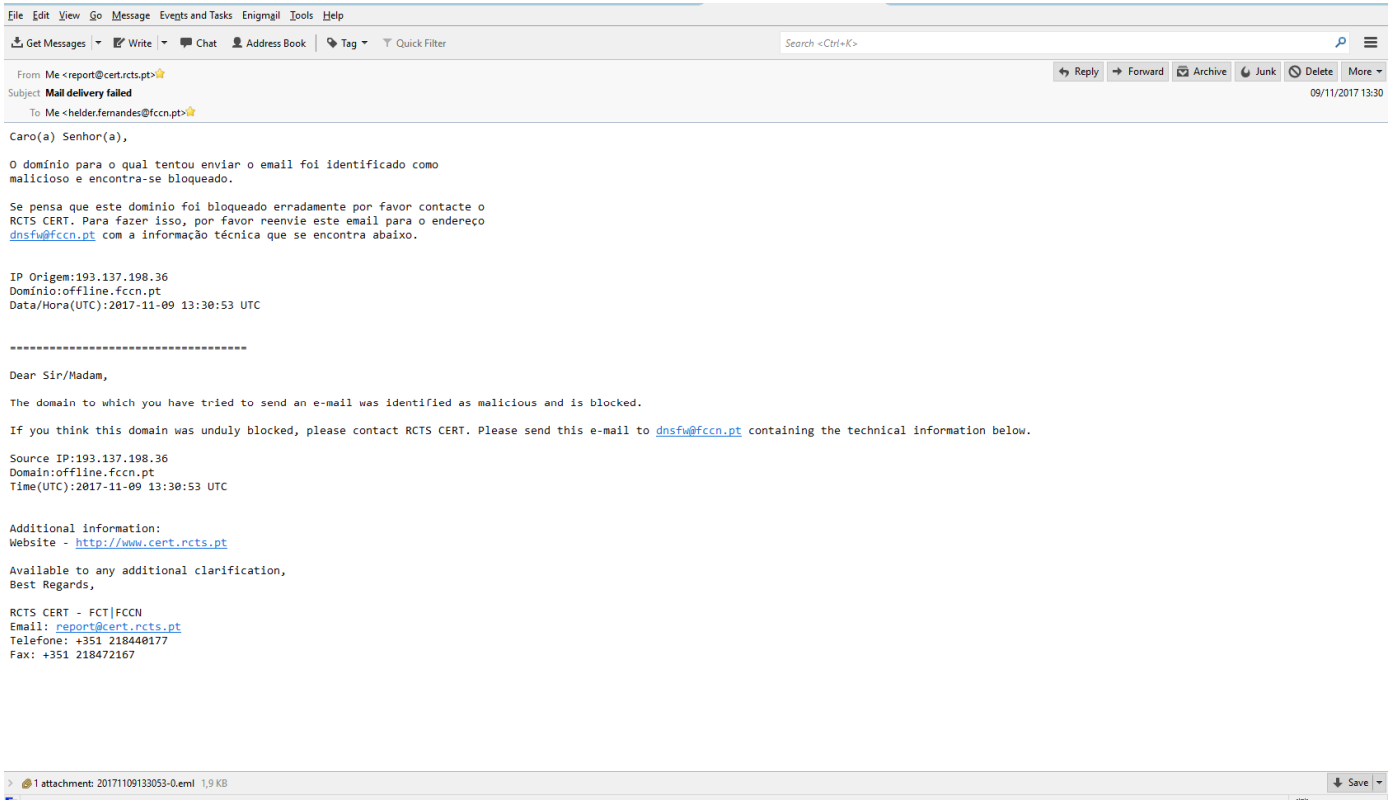
Landing Page



SMTP Sink


INTELMQ
Landing page logs
5
4
Resolver logs
Landing Page
Logs
Resolver
Bad domain email message
2
Landing page IP address response
3
Send email
Malicious domain query
1

Aviso de não entrega



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>

Reply | Forward | Archive | Junk | Delete | More

09/11/2017 13:30

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
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

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

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

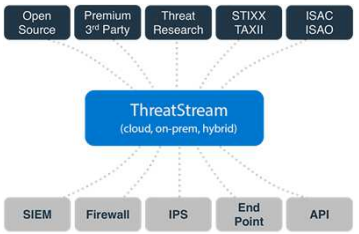
Falsos Positivos

- 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

Conclusões

- O verdadeiro **desafio** está na gestão dos feeds
- É muito importante manter a lista de domínios **atualizada** de forma a garantir a menor quantidade possível de falsos positivos e falsos negativos
- **Cooperar** e manter a informação sobre os domínios maliciosos acessível a todos
- Focar em domínios que têm como objetivo atacar o **ciberespaço nacional**



Obrigado

Pedidos de adesão: **dnsfw@fccn.pt**