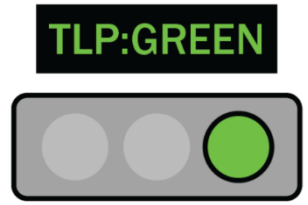


RNEP-GW

MÓDULO DNS FIREWALL

fct csirt

RNEP-GW

DNS FIREWALL

OBJECTIVO

Impedir (fases de) processos de infecção

Como?

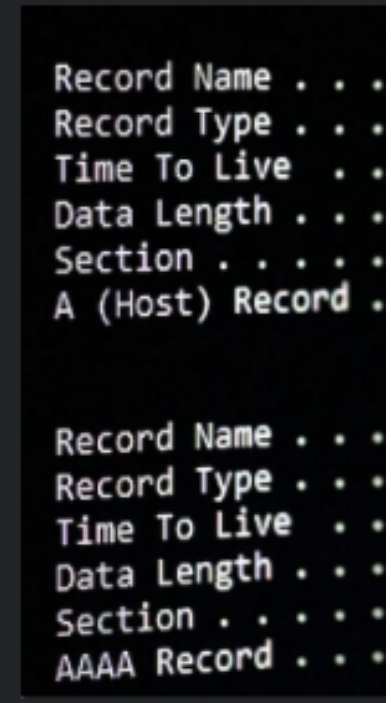
- Desviando o acesso a domínios classificados como maliciosos através do DNS
- Manipulando as respostas dos DNS resolvers

IT'S ALWAYS DNS

Hackers exploit a blind spot by hiding malware inside DNS records

Technique transforms the Internet DNS into an unconventional file storage system.

DAN GOODIN – 16 JUL 2025 12:15 | 67

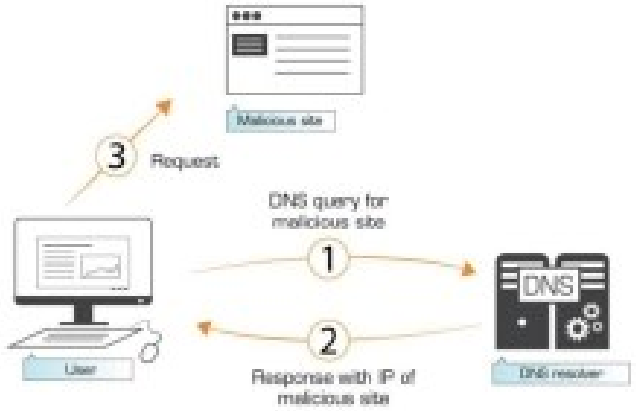


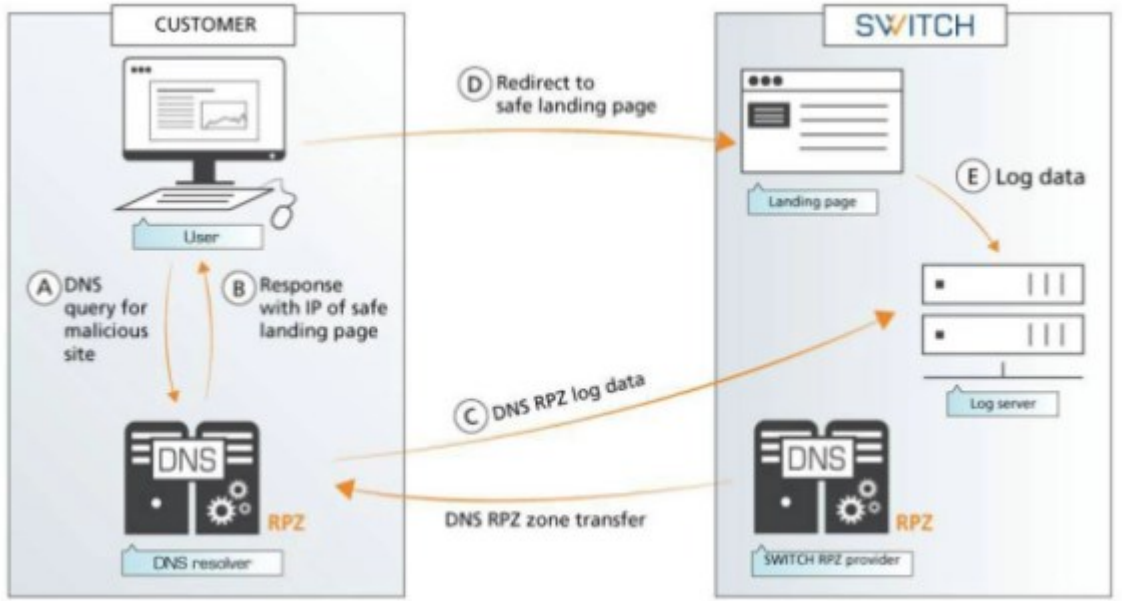
Screenshot Credit: G

Hackers are stashing malware in a place that's largely out of the reach of most defenses—inside domain name system (DNS) records that map domain names to their corresponding numerical IP addresses.

The practice allows malicious scripts and early-stage malware to fetch binary files without having to download them from suspicious sites or attach them to emails, where they frequently get quarantined by antivirus software. That's because traffic for DNS lookups often goes largely unmonitored by many security tools. Whereas web and email traffic is often closely scrutinized, DNS traffic largely represents a blind spot for such defenses.

INSPIRAÇÃO: SWITCH.CH





DADOS DE UTILIZAÇÃO

Ano	Milhões de Hits
2024	2.42
2023	1.20
2022	1.60
2021	2.76
2020	3.00
2019	3.90
2018	5.00

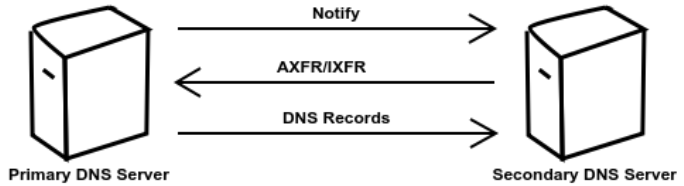
TIPOS DE UTILIZAÇÃO

12 instituições de forma directa

- Através do cluster resolver.fccn.pt

13 instituições através de DNS AXFR

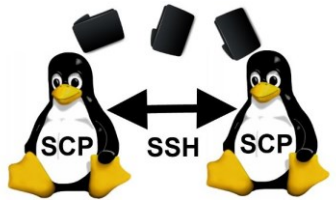
- Em resolver DNS próprio



Message flow between DNS Servers

7 instituições através de secure copy (scp)

- Instalação em resolver DNS próprio
- Podendo alterar ou não a «Landing Page»



TIPOS DE UTILIZAÇÃO

Disponibilizamos um «Cookbook» à nossa comunidade

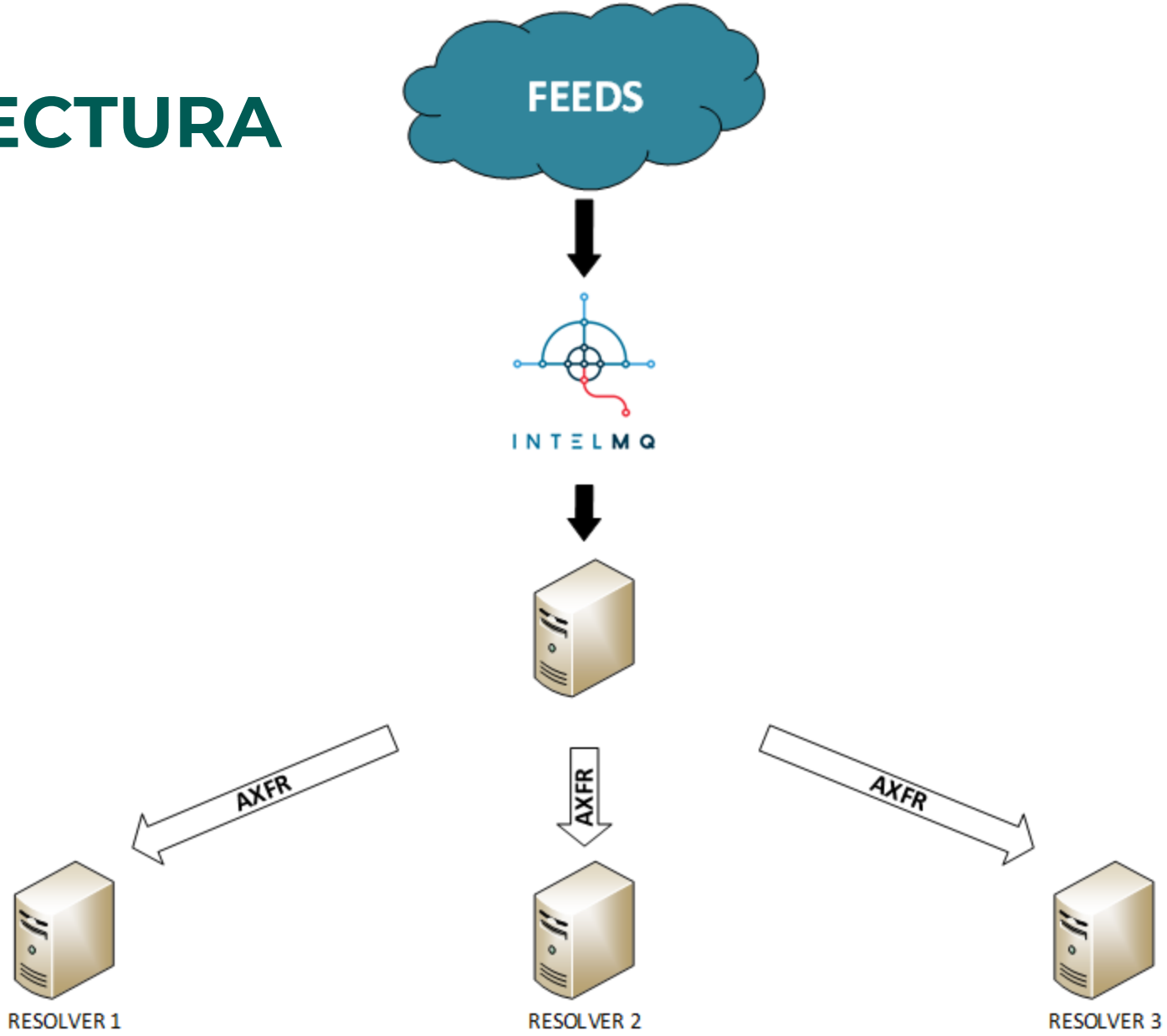
O uso directo é ativado apenas com a inserção das redes IP de uma instituição aderente na configuração BIND do nosso cluster DNS resolver

TIPOS DE UTILIZAÇÃO: DIFICULDADES

A utilização de resolvers DNS públicos de forma massiva

Diferentes departamentos têm políticas de utilização de resolvers DNS diferentes

ARQUITECTURA



FEEDS

Ioc2rpz-DGA (~940k)

ioc2rpz-Malware (~492k)

bambenek-dga-domains (~492k)

Fraunhofer-DGA (~478k)

kriskintel-maze-ransomware (~2k)

shadowserver (residual)

GESTÃO DA LISTA

Domain Blacklist 1.0

Total de dominios ->2443022

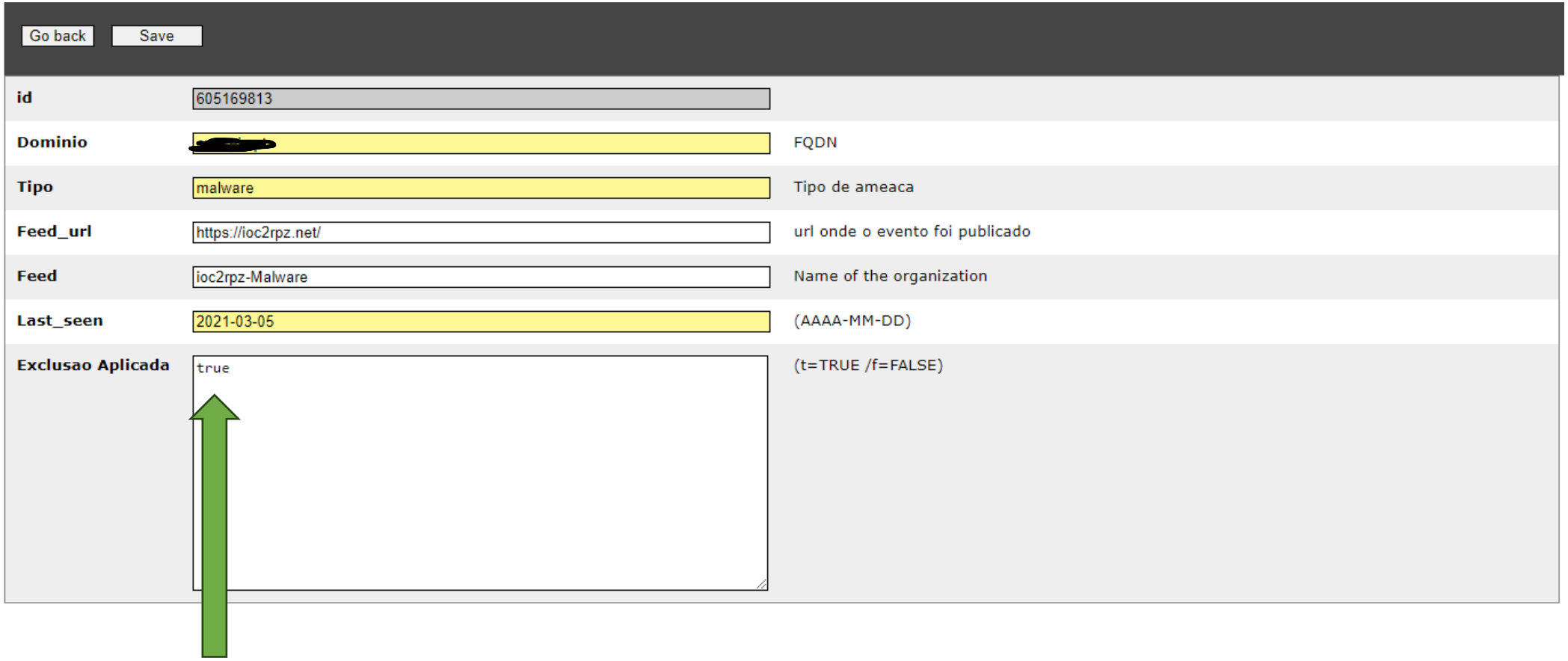
1 2 3 4 5 6 7 8 9 10 11 Next

Protect this directory with .htaccess

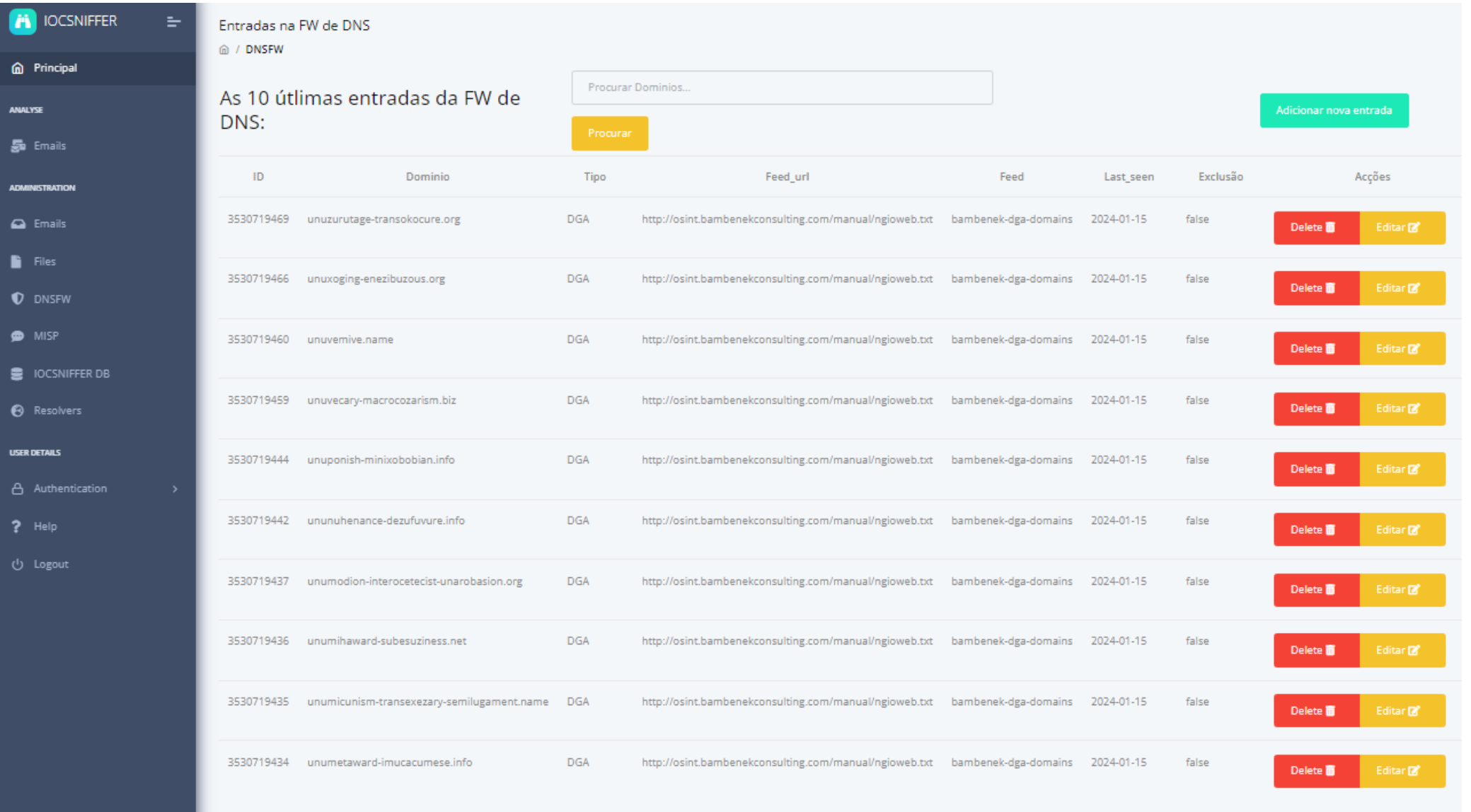
id Search Add Record

id	Dominio	Tipo	Feed_url	Feed	Last_seen	Exclusao Aplicada
3524273608	unuzurutage-transokocure.org	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false
3524273605	unuxoging-enezibuzous.org	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false
3524273599	unuvemive.name	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false
3524273598	unuvecary-macrocozarism.biz	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false
3524273583	unuponish-minixobobian.info	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false
3524273581	ununuhenance-dezufuvure.info	DGA	http://osint.bambenekconsulting.com/manual/ngioweb.txt	bambenek-dga-domains	2024-01-13	false

WHITELISTING



GESTÃO DA LISTA: INTERFACE «MODERNA»



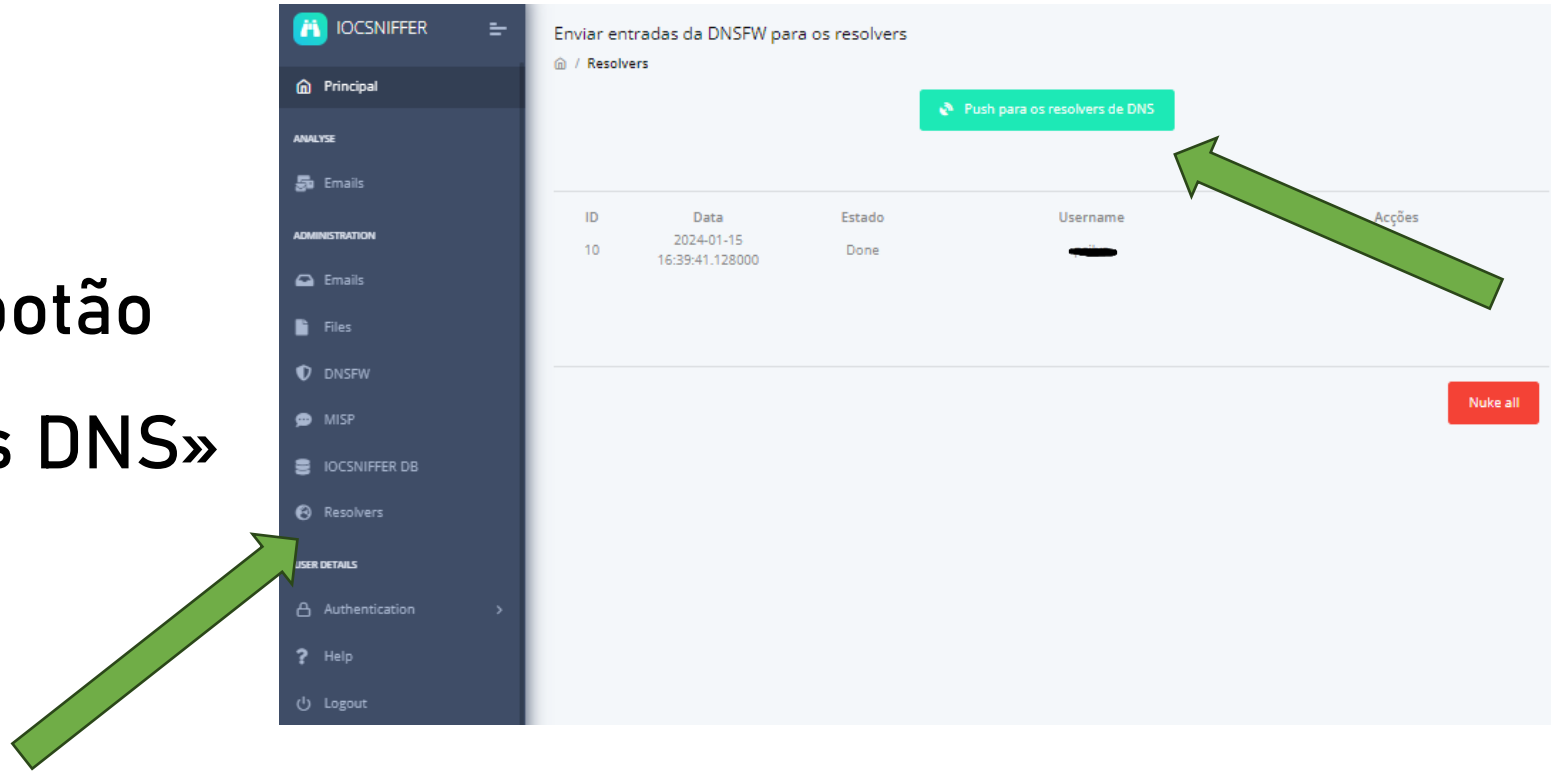
IMPORTAÇÃO DE IOCS «IN-HOUSE»

IOCSNIFFER

Menú “Resolvers”

Exportação através do botão

«Push para os resolvers DNS»



A LISTA

Constituída por duas zonas

- Domínios maliciosos (db.rpz)
- DGAs: Domain Generated Algorithms (dga.rpz)

Cada instituição pode optar por receber apenas uma, ou ambas

«LANDING PAGE»

«LANDING PAGE»

Offline.fccn.pt

- É este o nome associado na zona RPZ gerada/disponibilizada

É indicado o endereço dnsfw@fccn.pt para reportar falsos positivos

- Que são raros (~10 por ano)

«BOUNCING» EMAILS

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**
To Me <helder.fernandes@fccn.pt>
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 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:[redacted]
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:[redacted]
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

SUMÁRIO

Em funcionamento desde Dezembro/2017

32 instituições ligadas à RCTS a usar o serviço (em 94)

Lógica de OPT-IN

Lista actual com cerca de 2.53 milhões de domínios

Poucos falsos positivos

REFERÊNCIAS

https://dnsrpz.info/

https://blogs.cisco.com/security/using-dns-rpz-to-block-malicious-dns-requests

https://www.switch.ch/en/dns-firewall

https://ioc2rpz.net/

https://osint.bambenekconsulting.com/feeds/

https://dgarchive.caad.fkie.fraunhofer.de/

IDEIAS CHAVE

- A utilidade está na prevenção de infecções cujos processos recorram ao DNS
- O tamanho da lista de domínios maliciosos é importante
- A «landing page» é um elemento essencial

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc