

FCT

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

FCCN

Computação
Científica Nacional

DNS FIREWALL User Cookbook



Julho 2019
v1.3

WWW.FCCN.PT

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

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

Pedido de ativação: dnsw@fccn.pt

Linux, /etc/resolv.conf

nameserver 193.136.192.45

nameserver 2001:690:a00:4001::100

(se existir conectividade IPv6)

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.

- Pedido (para dnsw@fccn.pt) indicando endereço IP que receberá a informação
 - Username
 - Password
 - Ou em alternativa instalação de chave pública
 - Path/Caminho
- AXFR da zona RPZ
 - Indicar o endereço IP do servidor DNS

- ❑ A exportação da zona ocorre todos os dias às **6:30**

- ❑ O endereço IP que inicia o scp (secure copy) é o **193.137.47.139**
 - ❑ Ligação ao porto 22 do Sistema da instituição deverá ser permitido

❑ ssh-rsa

```
AAAAB3NzaC1yc2EAAAADAQABAAQBAQC0wx+V7l3Fwj  
XNkWxrtxGKJcecp0uKH6GL3o2hMQ+kK585L+B+qH0ok  
3fYBwPbhCY8GyQcZ0bKAKHJRJB6T+vpWPXsJ0cqkQ/rR  
LiF5oVbYkwZP4df0j3OmST81zd7pbBrl9wuFQOafQqLw  
0+fdhwvDUnDJf6WisZhrGpLy+aDWbdhKoDuki4OkcbTZ  
UzB9mnav18LmpmikaRFdDs/yPkdMcLN93XZopEyQSS/  
rFIMpiFR/F390czMwgsjcGg/cF8uFh8XoPa522gB3uh1Fv  
9nk/t0oVOZHgK+nyDhlc0A3DWQ/dak3W1zv/ps65wcP  
XVITH0BZdPHyYB7+PBgL2K3 rpzuser
```

□ /etc/named.conf

```
options {
    response-policy {
        zone "malware";
        zone "malware.dga";
    };
};
#Chave de segurança para permitir transferencia de zona
key fccnkey {
    algorithm hmac-sha256;
    secret "chave enviada por email";
};
masters fccn-rpz-master {
    //rpzmaster.cert.rcts.pt
    193.136.192.143 key fccnkey;
};
```


❏ /etc/named.conf

#Zonas a transferir por AXFR

```
zone "malware" {  
    type slave;  
    file "slaves/fccn_malware.zone";  
    allow-notify { 193.136.192.143; };  
    masters { fccn-rpz-master; };  
};  
  
zone "malware.dga" {  
    type slave;  
    file "slaves/fccn_malware.dga.zone";  
    allow-notify { 193.136.192.143; };  
    masters { fccn-rpz-master; };  
};
```

□ /etc/named.conf

#Ficheiro de logs com os Hits

```
logging {  
    channel named-rpz {  
        file "/var/log/bind/rpz.log" version 3 size 250k;  
        Severity info;  
    };  
    category rpz { named-rpz; };  
};
```

- ❑ `offline.fccn.pt` e `193.137.196.12` estão embutidos na zona gerada (`db.rpz`)
- ❑ Em Linux, pode-se fazer facilmente parsing ao ficheiro `db.rpz`, para substituir esse endereço:

```
cat db.rpz | sed -e "s/193.137.196.12/10.0.0.1/g" | sed -e "s/offline.fccn.pt/offline.mydomain.pt/g"
```

- ❑ E naturalmente redirecionar o output desse comando para um novo ficheiro de zona, a usar no ISC BIND

- É importante analisar os *logs* da «landing page».
- Pode-se recolher informação muito útil para melhor compreender e combater o *malware*.
- A FCCN está interessada nestes dados.

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

- ❑ <https://dnssrpz.info>
- ❑ <https://www.isc.org/rpz/>

Obrigado

dnsw@fccn.pt