DNS FIREWALL
USER COOKBOOK

Outubro 2023
v1.5

FCCN UNIDADE DA FCT

fct Fundação para a Ciência e a Tecnologia

DNS FIREWALL @RCTS: COMO?

- 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

OPÇÃO I

- Pedido de ativação: dnsfw@fccn.pt

- Linux, /etc/resolv.conf
  - nameserver 193.136.192.45
  - nameserver 2001:690:a00:4001::100

    (se existir conectividade IPv6)

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.

OPÇÃO II

- Pedido (para dnsfw@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

OPÇÃO II

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

- O endereço IP que inicia o scp (secure copy) é o 193.136.47.195
  - Ligação ao porto 22 do Sistema da instituição deverá ser permitido

OPÇÃO II, CHAVE PÚBLICA

- ssh-rsa
  AAAAB3NzaC1yc2EAAAADAQABAAABAQC0wx+V7l3FwjXNkWxrtxGKJce
  cp0uKH6GL3o2hMQ+kK585L+B+qHOok3fYBwPbhCY8GyQcZ0bKAKHJRJ
  B6T+vpWPXsJ0cqkQ/rRLiF5oVbYkwZP4df0j3OmST81zd7pbBrI9wuFQOa
  fQqLw0+fdhwvDUnDJf6WisZhrGpLy+aDWbdhKoDuki4OkcbTZUZB9mna
  v18LmpmikaRFdDs/yPkdMcLN93XZopEyQSS/rFlMpiFR/F390czMwgsjcG
  g/cF8uFh8XoPa522gB3uh1Fv9nk/t0oVOZHGK+nyDhic0A3DWQ/dak3W
  1zv/ps65wcPXVITH0BZdPHyYB7+PBgL2K3 rpzuser

OPÇÃO II, ISC BIND

❑ /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;
};
```

OPÇÃO II, ISC BIND

❑ /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; };
};
```

OPÇÃO II, ISC BIND

❑ /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; };
};
```

OPÇÃO II, «LANDING PAGE»

- 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

OPÇÃO II, «LANDING PAGE»

- 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.

FALSOS POSITIVOS

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

REFERÊNCIAS

- https://dnsrpz.info
- https://www.isc.org/rpz
- https://www.cert.rcts.pt/pt/sobre/servicos
- https://www.circleid.com/posts/20100728_taking_back_the_dns
- https://abuse.ch/blog/using-urlhaus-as-response-policy-zone-rpz

CERT RCTS

Obrigado

dnsfw@fccn.pt

FCCN UNIDADE DA FCT

fct Fundação para a Ciência e a Tecnologia