DNS FIREWALL

Hélder Fernandes

Helder.fernandes@fccn.pt

Patrocinadores **Platina**

Patrocinadores **Ouro**

Patrocinadores **Prata**

Apoios

Organização

DNS FIREWALL: O que é?

- **D**omain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones
    - Desenvolvido por Internet Systems Consortium
    - Disponibilizado em 2010 através do BIND versão 9.8.1
- A.k.a <<DNS Firewall>>

(Ilustração por Christoph Frei)

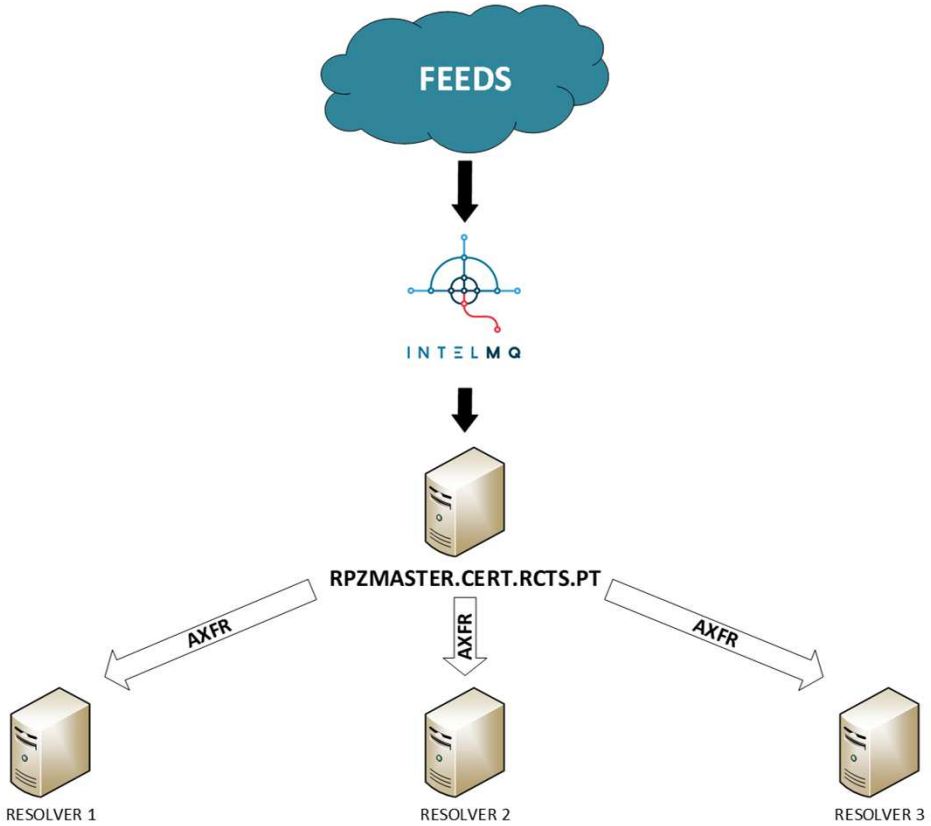
DNS FIREWALL: Características

- Bloquear o acesso a domínios classificados como maliciosos (Zona RPZ)
- O bloqueio é efetuado através da manipulação das respostas dos DNS resolvers
- Mecanismo de auxílio no combate a:
  - Phishing
  - Código malicioso

DNS FIREWALL: O que é um domínio malicioso?

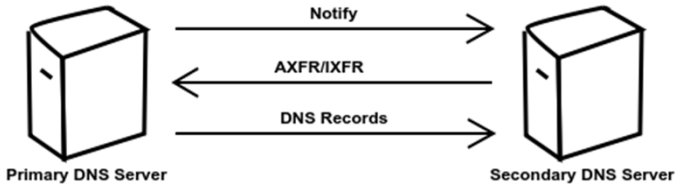
- update-apple.com.betawihosting.net
- secured-microsoftonline.000webhostapp.com
- yifruktpo.ru
- qgzgafeiqtf.info

DNS FIREWALL: Arquitectura



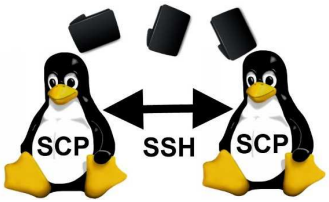
DNS FIREWALL: Distribuição de Zona

- Automática:
  - Transferência de Zona via AXFR



Message flow between DNS Servers

- Manual
  - Cópia da zona RPZ via SSH



DNS FIREWALL: Feeds

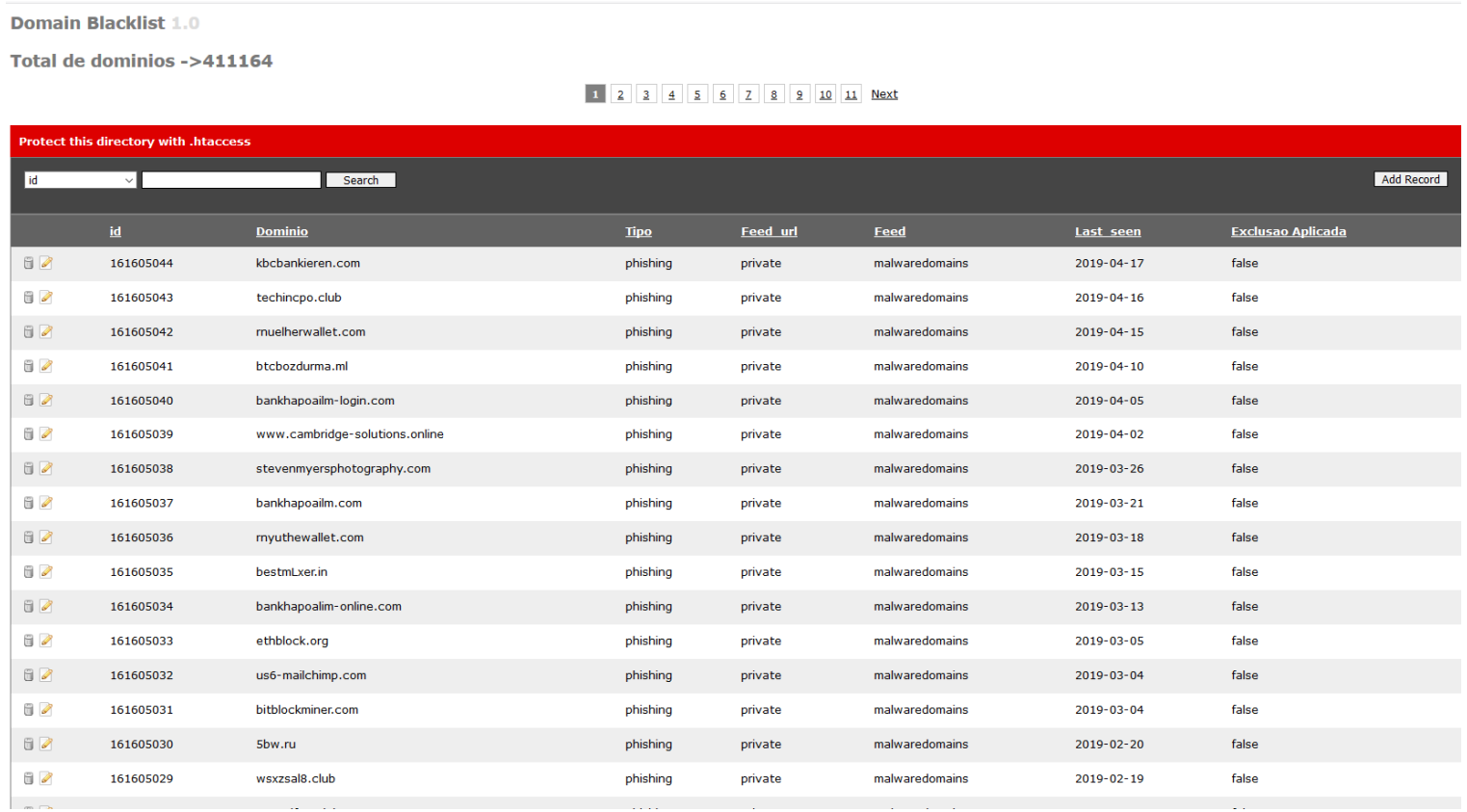
- Várias fontes, gratuitas
- 410.000 domínios maliciosos

- Análise de Malware
  - IoCs adicionados pelo RCTS CERT
  - Utilização de ferramentas, como o Cuckoo ou FLARE VM
  - Aberto a IoCs de outros CSIRTs

cuckoo

FLARE

DNS FIREWALL: Gestão de Feeds



Domain Blacklist 1.0

Total de dominios ->411164

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

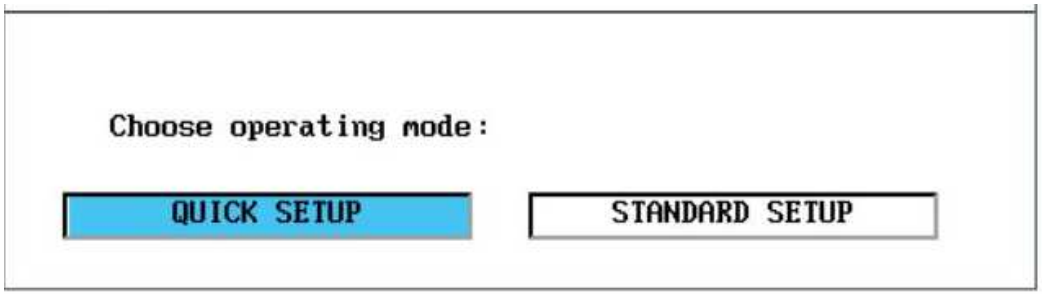
Protect this directory with .htaccess

id Search Add Record

id	Dominio	Tipo	Feed_url	Feed	Last_seen	Exclusao Aplicada
161605044	kbcbankieren.com	phishing	private	malwaredomains	2019-04-17	false
161605043	techincpo.club	phishing	private	malwaredomains	2019-04-16	false
161605042	rnuelherwallet.com	phishing	private	malwaredomains	2019-04-15	false
161605041	btcbozdurma.ml	phishing	private	malwaredomains	2019-04-10	false
161605040	bankhapoailm-login.com	phishing	private	malwaredomains	2019-04-05	false
161605039	www.cambridge-solutions.online	phishing	private	malwaredomains	2019-04-02	false
161605038	stevenmyersphotography.com	phishing	private	malwaredomains	2019-03-26	false
161605037	bankhapoailm.com	phishing	private	malwaredomains	2019-03-21	false
161605036	rnyuthewallet.com	phishing	private	malwaredomains	2019-03-18	false
161605035	bestmLxer.in	phishing	private	malwaredomains	2019-03-15	false
161605034	bankhapoalim-online.com	phishing	private	malwaredomains	2019-03-13	false
161605033	ethblock.org	phishing	private	malwaredomains	2019-03-05	false
161605032	us6-mailchimp.com	phishing	private	malwaredomains	2019-03-04	false
161605031	bitblockminer.com	phishing	private	malwaredomains	2019-03-04	false
161605030	5bw.ru	phishing	private	malwaredomains	2019-02-20	false
161605029	wsxzsal8.club	phishing	private	malwaredomains	2019-02-19	false

DNS FIREWALL: Opções de utilização

- Utilização dos Resolvers da RCTS
- Utilização de resolvers próprios
  - Distribuição de zona através de cópia ssh
  - Distribuição de zona via AXFR



DNS FIREWALL: <<Landing Page>>

FCT Fundação para a Ciência e a Tecnologia | 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

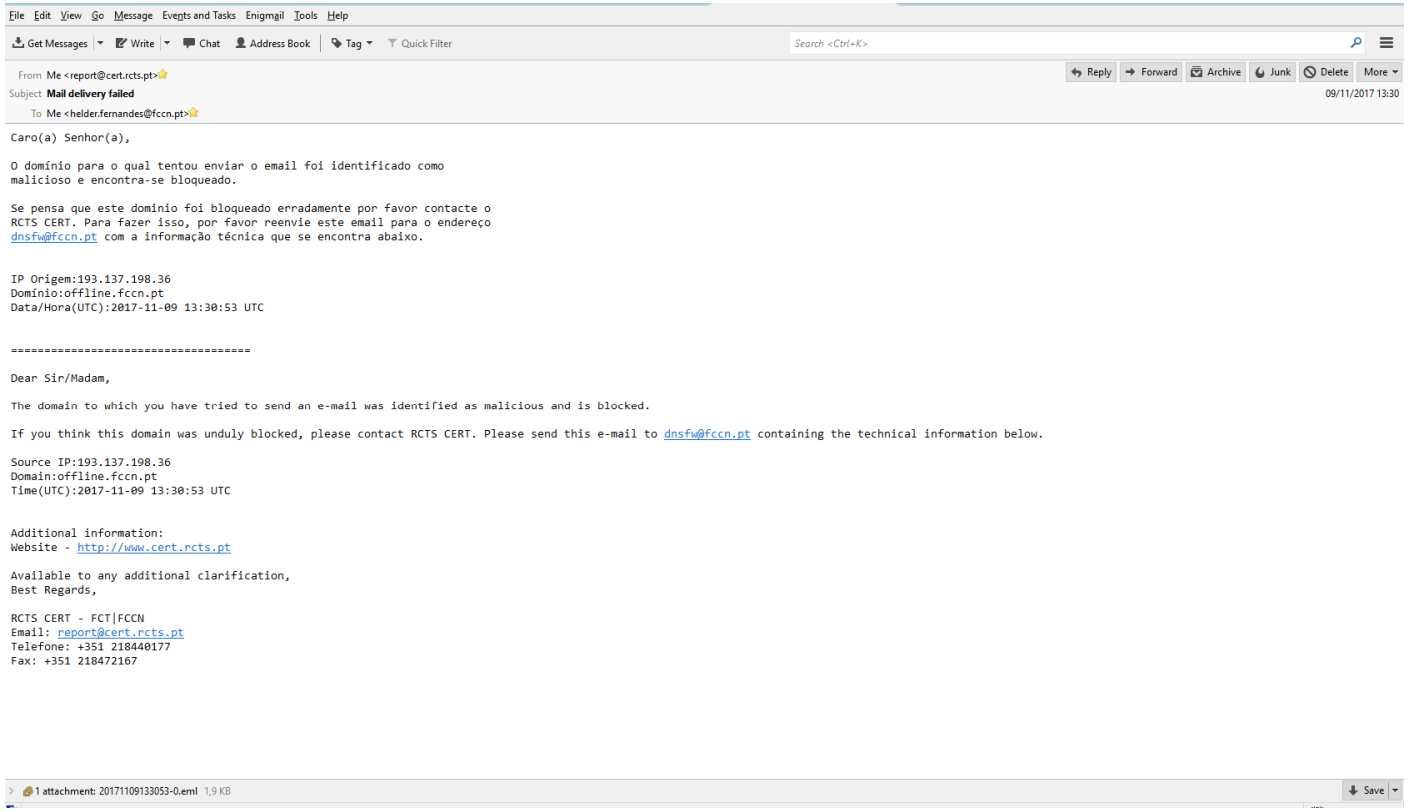
Se pensa que esta pagina foi bloqueada erradamente por favor contacte o RCTS CERT. Para fazer isso, adicione ao email a informação técnica que se encontra abaixo, bem como uma pequena descrição do motivo pelo qual o domínio deve ser desbloqueado . O email deve ser enviado para dnsfw@fccn.pt

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 FIREWALL: <<Bounce>>



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 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: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

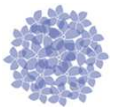
1 attachment: 20171109133053-0.eml 1,9 KB | Save

DNS FIREWALL: Falsos positivos

- O interface permite excluir domínios, de forma manual, se necessário
- Atualização manual de zona em caso seja necessário
- É importante comunicar os falsos positivos
  - dnsfw@fccn.pt

É importante recebermos os logs do RPZ para um melhor controlo dos falsos positivos!!

DNS FIREWALL: Adesão ao serviço



FCT Fundação para a Ciência e a Tecnologia
Computação Científica Nacional
FCCN

POLITÉCNICO DE LISBOA

utad UNIVERSIDADE DE TRÁS-OS-MONTES E ALTO DOURO

IPCA INSTITUTO POLITÉCNICO DO CÁVADO E DO AVE

RAE
Rede Alargada da Educação

Instituto Politécnico de Castelo Branco

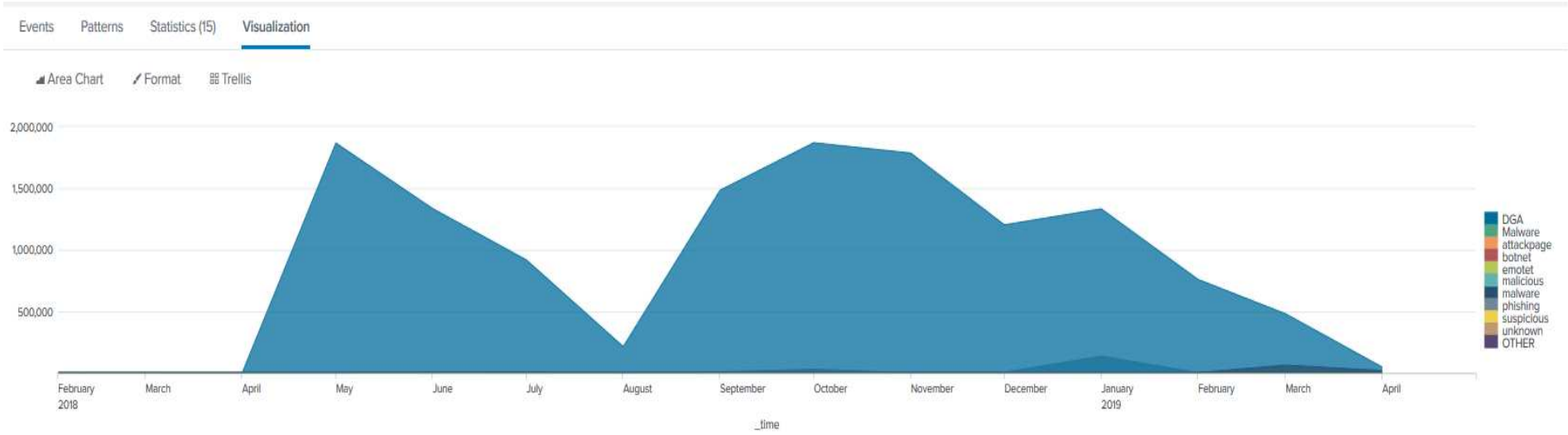
U.PORTO

ipt Instituto Politécnico de Tomar

DNS FIREWALL: Resultados

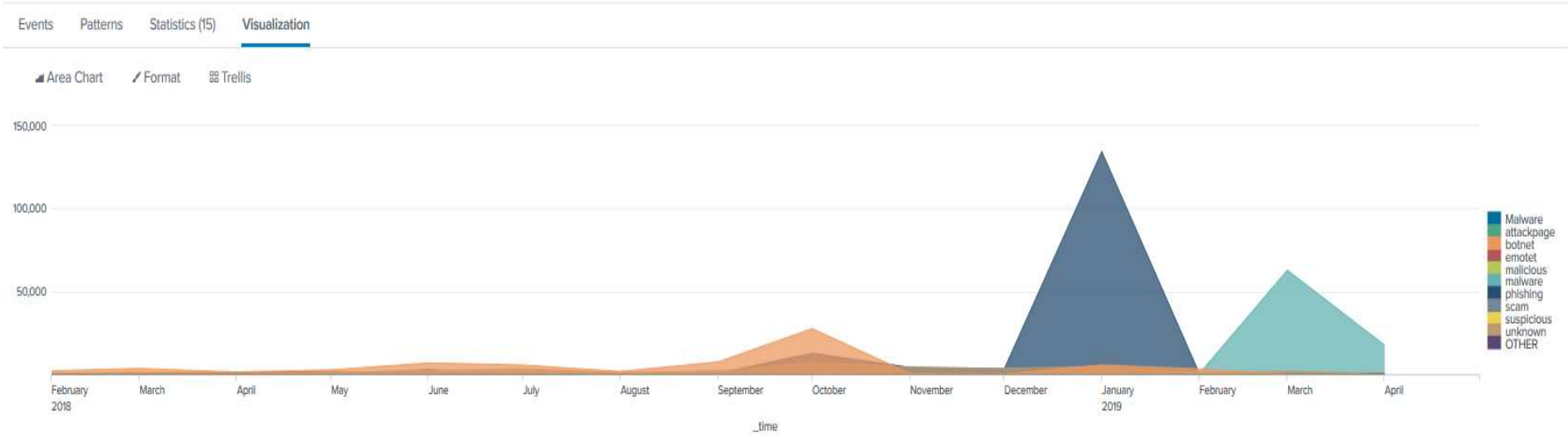
13.494.115 eventos desde Fevereiro de 2018

- **13.166.120 são referentes a domínios DGA**
- **2.020 domínios bloqueados**



DNS FIREWALL: Resultados

Resultados sem contabilizar domínios do tipo DGA
“*domain generation algorithm*”



DNS FIREWALL: Desafios

- Continuação da divulgação do serviço

- Aumentar o número de domínios a bloquear

- Melhorar continuamente o sistema de reporting
    - Eventos agora incluídos nos relatórios semanais

DNS FIREWALL: Aderir

dnsfw@fccn.pt

DNS FIREWALL: Questões

Obrigado