



IOCSNIFFER



Pedro Silva

02 de Junho de 2022



AGENDA

- **Âmbito**
- **IOCsniffer**
- **Arquitectura**
- **Vídeo demonstrativo**
- **A desenvolver**

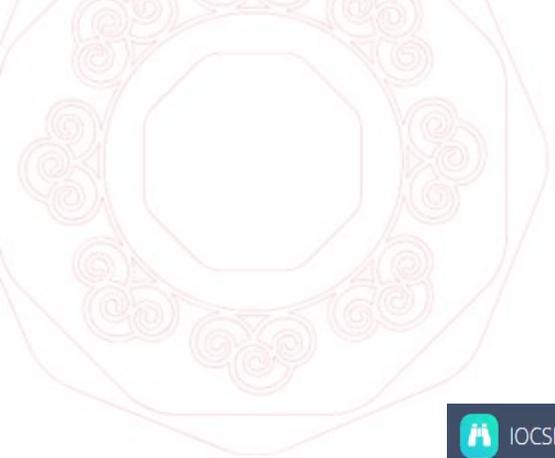




ÂMBITO

- **Porque foi criado?**
- **O que é?**
- **O que faz?**
- **Quem pode usar?**





IOCSNIFFER

IOCSNIFFER

Principal

ANALYSE

Emails

ADMINISTRATION

Emails

Files

DNSFW

MISP

IOCSNIFFER DB

Resolvers

USER DETAILS

Authentication

Help

Logout

pedro

What do I have to analyse today?



CONFIGURAÇÕES DE CADA UTILIZADOR

- **Dados do Utilizador**
- **Dados para o IOCSniffer**
- **Serviço de email**

Dados do Utilizador:

Nome: Pedro Silva

Username:

Email: pedro.silva@fccn.pt

Dados para o IOCSNIFFER:

Inbox: INBOX/

Editar

Email: seguranca@fccn.pt

Editar

Serviço de email:

Endereço:

Porta:

SSL:

STARTTLS:

Guardar



ANALIZAR EMAILS DE UTILIZADORES 1/2

- **Analisar**
- **Procurar**

User Inbox
🏠 / Email Box - Pedro Silva

Emails Recebidos:

Data: 2022-05-10

ID	Assunto	Flags	Acções
38680	RE: Threat Intel: Exposed multiple package/composer JSON Files	🔍 📧	Analisar 🔍
38698	RE: Threat Intel: Exposed multiple package/composer JSON Files	🔍 📧	Analisar 🔍
38707	Indisponibilidade temporária do sistema picagem - tarde 10/5	📧	Analisar 🔍

mm/dd/yyyy 🗒

[Procurar](#)



ANALIZAR EMAILS DE UTILIZADORES 2/2

- Analisar 1 email...

Home / Email Box Pedro Silva / Analyse 38680

- **Aparentemente Seguro**

Home / Email Box Pedro Silva / Analyse 606

- **Suspeito** Analisado.

- **Malicioso** Malicioso

O email foi classificado como Malicioso .
Por favor ignore, este email foi usado para algum tipo de esquema ilícito.



Analistas EMAILS

Home / Email Box Pedro Silva / Email 6666 / Raw 6666

Enviar Email: ✕

Tipo de resposta:

Escolher...
Escolher...
Seguro
Suspelo
Malicioso

Enviar Email Fechar

Email

Email 608

HEADERS BODY ATTACHMENTS

Domains

Acções

s3.amazonaws.com				
emails.jotform.com				
link.jotform.com				
www.w3.org				
www.youtube.com				
cdn.jotfor.ms				
tourisurf.com				

ADMINISTRATION

Emails

Files

DNSFW

MISP

IOCSNIFFER DB

Resolvers



Analistas FILES

ADMINISTRATION

- Emails
- Files** ←
- DNSFW
- MISP
- IOCSNIFFER DB
- Resolvers

Analisar Ficheiros

5b15 / File / malware.123

Domains	Acções
ynvj.kp	DNSFW IOCSniffer Misp
lkcbggy	DNSFW IOCSniffer Misp
ecru.sm	DNSFW IOCSniffer Misp
5rha.ml	DNSFW IOCSniffer Misp
u.ls	DNSFW IOCSniffer Misp
lnwg.se	DNSFW IOCSniffer Misp
oqsp.uz	DNSFW IOCSniffer Misp
gwjr.jp	DNSFW IOCSniffer Misp

Alibaba



Analistas DNSFW

ADMINISTRATION

Emails

Files

DNSFW 

MISP

IOCSNIFFER DB

Resolvers

Entradas na FW de DNS

/ DNSFW

Procurar Domínios...

Procurar

As 10 últimas entradas da FW de DNS:

Adicionar nova entrada ao DNSFW:

Domínio:

Tipo: phishing

Feed URL: Pedro Silva

Feed: RCTS

Exclusão: False

Data: mm/dd/yyyy

Adicionar nova entrada

Guardar

Fechar

ID	Domínio	Tipo	Feed_u	Exclusão	Acções		
1876129137	xx6a706c06.ru	DGA	dgarchive.caad.fkie.fraunhofer.de	Fraunhofer-DGA	2022-05-10	false	Delete  Editar 
1876129136	xx83603353.it	DGA	dgarchive.caad.fkie.fraunhofer.de	Fraunhofer-DGA	2022-05-10	false	Delete  Editar 



Analistas Resolvers

ADMINISTRATION

- Emails
- Files
- DNSFW
- MISP
- IOCSNIFFER DB
- Resolvers** ←

Enviar entradas da DNSFW para os resolvers

🏠 / Resolvers

Enviar entradas da DNSFW para os resolvers

🏠 / Resolvers

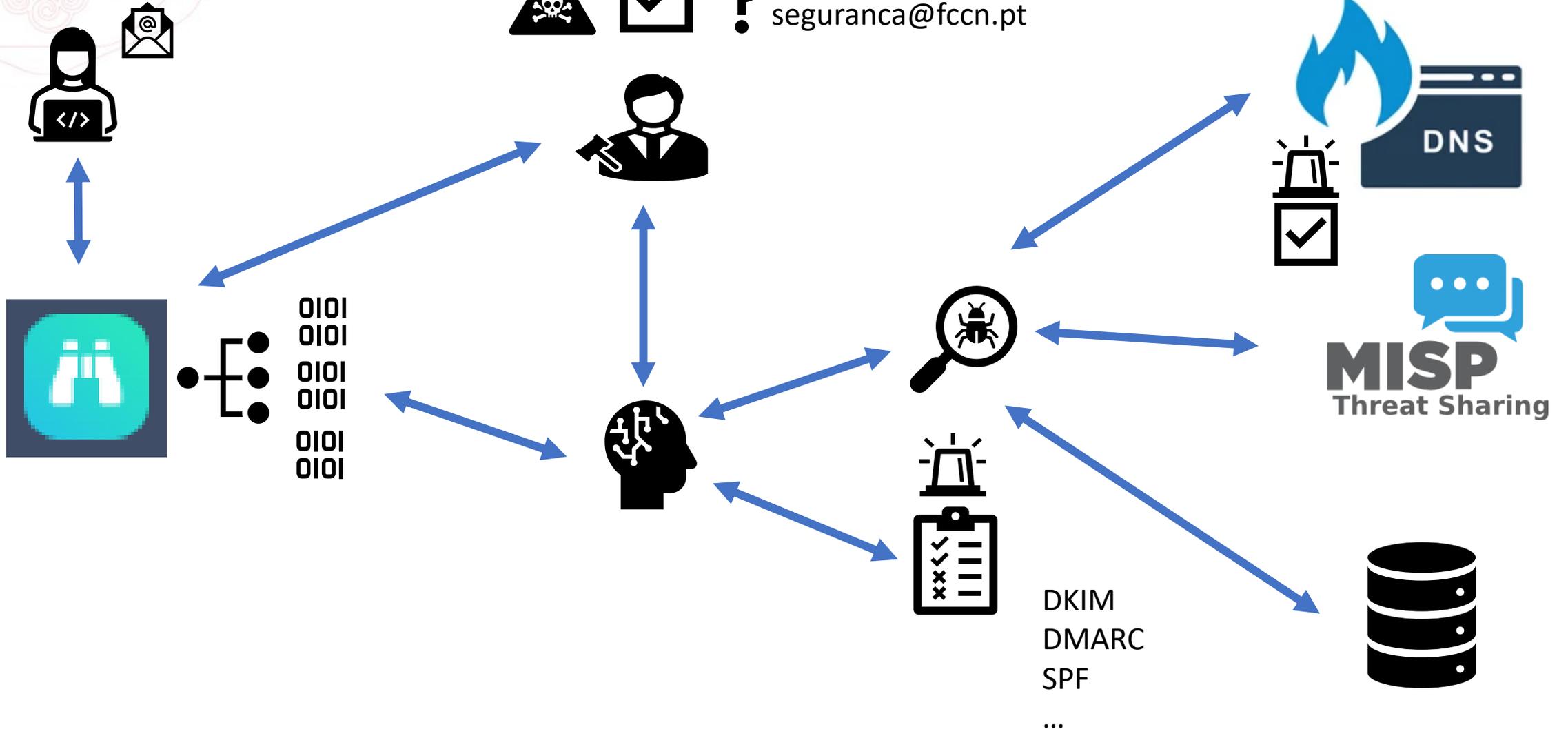
📡 Push para os resolvers de DNS

ID	Data	Estado	Username
4	2022-03-15 15:46:52.217490	Error	
5	2022-03-15 15:51:12.230912	Done	
6	2022-03-22 17:33:26.128694	Error	
7	2022-03-22 17:33:35.340998	Error	
8	2022-03-22 17:33:51.631687	Error	
9	2022-03-22 17:34:07.151177	Error	
10	2022-03-22 17:36:41.543507	Error	
11	2022-03-22 17:38:16.126566	Error	
12	2022-03-23 10:11:25.841714	Done	
13	2022-03-25 12:22:48.474212	Done	
14	2022-04-13 08:17:03.466827	Done	
15	2022-04-13 09:15:47.919094	Done	
16	2022-04-20 13:38:02.985103	Done	

Arquitectura



☠️ ☑️ ? seguranca@fccn.pt





Vídeo Demonstrativo

Activities Google Chrome

quá, 12 de mai 09:42

26,235.00 € en 100%

IOCSNIFFER

Not secure

incognito

Lock

Login

Username

Password

Login

KAPWING



A DESENVOLVER

-  **Autenticação Federada**
-  **Configurar Serviço de Email**
-  **Adicionar mais lógica**
-  **Multiprocessing**
-  **Melhorar a página de ajuda**
-  **Análise de ficheiros/anexos**
-  **Estatísticas**



Obrigado!

