jornadas FCCN

Serviços RCTS CERT

Carlos Friaças, Filipa Macieira, João Machado,
Louise Altvater, Pedro Silva

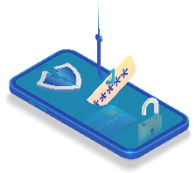
jornadas.fccn.pt

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | arditi agência regional para o desenvolvimento da investigação tecnologia e inovação | SIH | UNIVERSIDADE da MADEIRA

SERVIÇOS RCTS CERT

Tratamento de Incidentes

Auditorias



Campanhas de Phishing

DNS Firewall

Gestão de Vulnerabilidades

IOCaaS

QUEM TEM ACESSO?

RCTS

REDE CIÊNCIA, TECNOLOGIA E SOCIEDADE

TRATAMENTO DE INCIDENTES

Ponto de contacto para a RCTS

Coordenação com as equipas locais

Triagem

Abertura de caso

Classificação, de acordo com Taxonomia da RNCSIRT

Fecho de caso

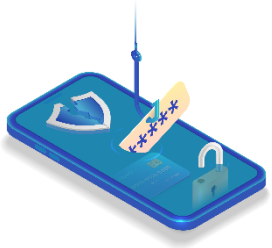
AUDITORIAS

Identificar vulnerabilidades, categorizadas em 3 níveis (alto, médio e baixo)

Geralmente sobre websites ou APIs

Produção de relatório

CAMPANHAS DE PHISHING



Alguns princípios base:

- Registo de domínio e uso de certificado SSL
- Não usar marcas reais
- Deixar sempre alguma pista de que se trata de uma fraude
- Não identificar quem introduz dados, apenas contar quantas pessoas o fazem
- Produção de relatório a descrever todo o desenho da campanha

DNS FIREWALL

~2.5 milhões de domínios

Lista de domínios de malware

Lista de domínios DGA (domain generation algorithm)

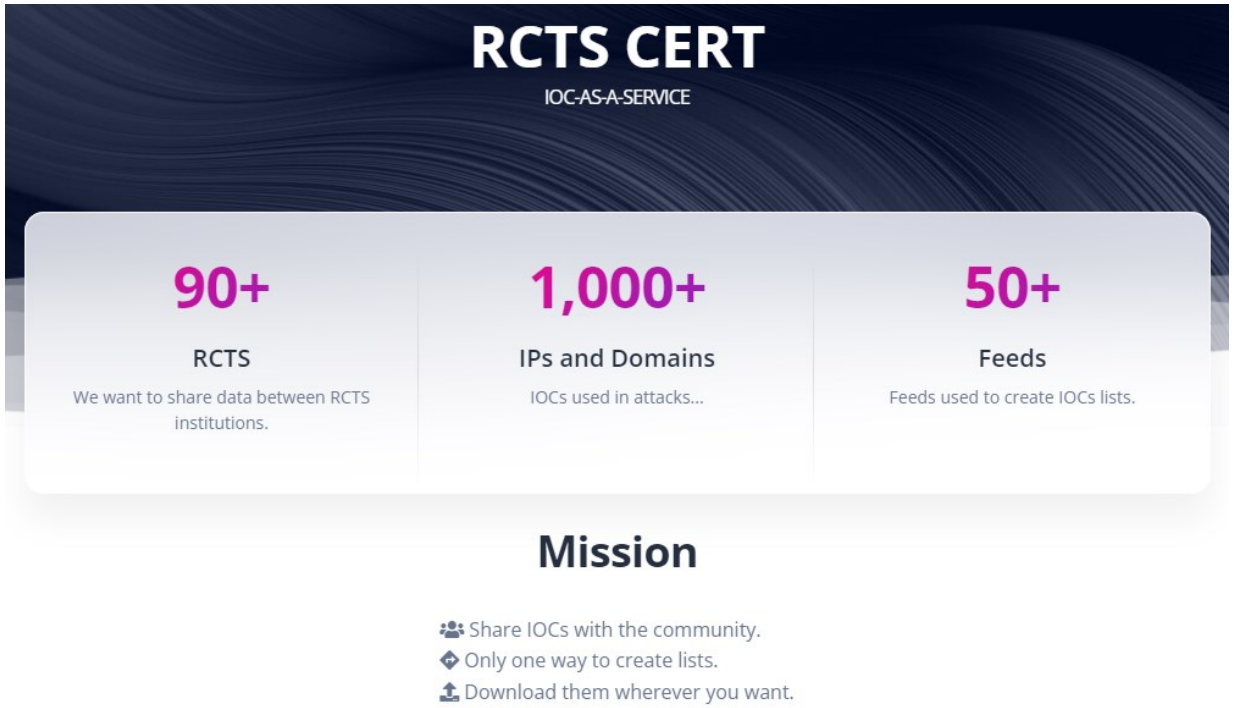
Redireccionamento para offline.fccn.pt

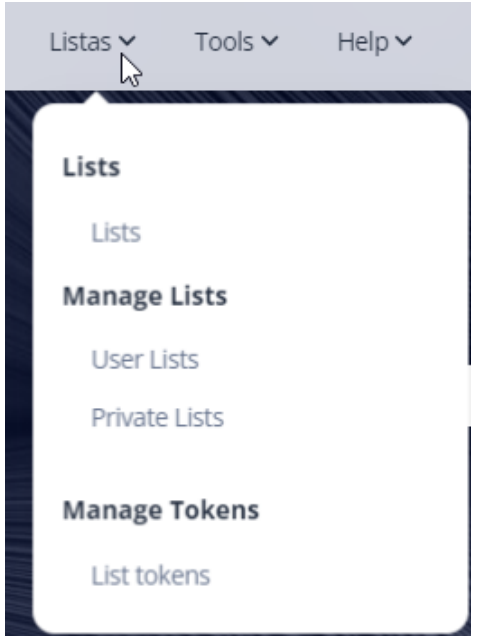
GESTÃO DE VULNERABILIDADES

Nessus® vulnerability scanner

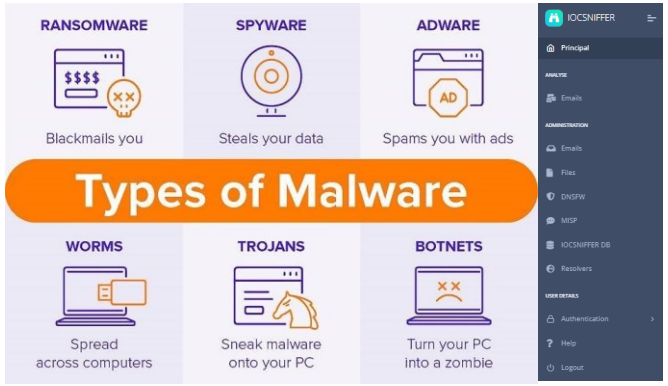
CVSS COMMON VULNERABILITY SCORING SYSTEM

IOCaaS


RCTS CERT
IOC-AS-A-SERVICE
90+
RCTS
We want to share data between RCTS institutions.
1,000+
IPs and Domains
IOCs used in attacks...
50+
Feeds
Feeds used to create IOCs lists.
Mission
Share IOCs with the community.
Only one way to create lists.
Download them wherever you want.


Listas
Tools
Help
Lists
Lists
Manage Lists
User Lists
Private Lists
Manage Tokens
List tokens

OUTROS



CERT RCTS

SECURITY PORTAL

Here you can check:
- Incidents
- Statistics
- Events
- Blacklists
- Security Reports
- And much more...

Federated Login

LIR
Local Internet Registry

RIPE NCC MEMBER

CVSS
COMMON VULNERABILITY SCORING SYSTEM

Microsoft
cisco
WordPress
Joomla!
Apache
php

FCCN
fct Fundação para a Ciência e a Tecnologia
arditi
SIH
UNIVERSIDADE da MADEIRA

MÉTRICAS 2023

Eventos de segurança RCTS	2.719.025	Ataques DDoS	661	Análises de Malware	3041
Campanhas de Phishing	7	Auditorias	13	Alertas e Recomendações à Comunidade	17
Tratamento de Incidentes	350	Gestão de Vulnerabilidades	23	Eventos DNS Firewall	1.208.842
Envio de relatórios semanais	52	Queixas a redes externas	690	Endereços IPv4 distribuídos	4448

jornadas FCCN

Obrigado.

Discussão

jornadas.fccn.pt

FCCN serviços digitais fct | fct Fundação para a Ciência e a Tecnologia | arditi agência regional para o desenvolvimento da investigação tecnologia e inovação | SIH | UNIVERSIDADE da MADEIRA

jornadas FCCN

biblioteca do conhecimento online b-on

Happy Hour 20 Anos B-ON

Junte-se a nós no **Centro de Congressos** para um brinde comemorativo

jornadas.fccn.pt

FCCN serviços digitais fct

fct Fundação para a Ciência e a Tecnologia

arditi agência regional para o desenvolvimento da investigação tecnológica e inovação

SIH

UNIVERSIDADE da MADEIRA