Segurança Cibernética no Contexto de ccTLD

FORMAÇÃO “ECOSSISTEMA TÉCNICO, JURÍDICO E ADMINISTRATIVE DE UM CCTLD”

José Casinha, .PT
Vogal da Comissão Executiva

24.09.2025, Moçambique

Quem somos

- Registry do .pt, domínio de topo de Portugal
- Dinamizar e promover a utilização da internet a nível nacional
- Player nacional na capacitação e inclusão digital de pessoas e organizações
- Segurança e confiança no .pt

Contexto

O que é um ccTLDs?

Um ccTLD é um tipo de domínio de topo que representa um país específico. É como um "sobrenome" online que indica a origem geográfica de um site.

Os TLDs são classificados geralmente por:

- gTLD: Tais como .com; .org ou .amazon.
- ccTLD: Country Code Top Level Domain como é o .pt.

Ecossistema DNS

DNS em poucas palavras

Centro de Operações de Segurança

O Centro de Operações de Segurança do .PT – **PTSOC** – encerra dois grandes objetivos na sua atuação:

Acelerar e aprofundar internamente as capacidades de deteção, resposta e prevenção de incidentes de segurança e ameaças cibernéticas, dotando o .PT dos meios tecnológicos, processuais e humanos necessários à proteção da sua infraestrutura e serviços críticos.

Densificar os níveis de cooperação com os nossos parceiros, nomeadamente no contexto do ecossistema da gestão dos nomes de domínio.

Plano de resposta a incidentes

Plano de resposta a incidentes

Identificação

Compreender o contexto da organização, os processos que suportam as atividades críticas, conhecer os riscos de cibersegurança que a podem impactar e desenvolver estratégias para os prevenir e/ou mitigar.

Governação & Controlo

- Missão e Objetivos
- Framework
- Papéis e Responsabilidades

Gestão do Risco & *Compliance*

- Análise e tratamento dos riscos
- Requisitos mínimos de segurança
- Normativos e legislação aplicável

Auditoria

- Auditorias de segurança aos sistemas e redes
- Auditorias de compliance

Plano de resposta a incidentes

Proteção

Desenvolver e implementar controlos apropriados para garantir a segurança das atividades críticas, ou seja, neste contexto, são implementados mecanismos que limitem ou contenham o impacto de um potencial incidente de cibersegurança, através de ações de sensibilização realizadas aos colaboradores, partilha de informação de inteligência dentro da comunidade CSIRT

Awareness

- Ações de sensibilização
- Partilha de informação RNCSIRT

Protective Technologies

- Controlo de Perímetro (Firewalls)
- Segurança Endpoint (Antivírus)
- Filtro de e-mails anti-spam
- Controlo de Acessos e Backups

Cyber Intelligence

- Análise de relatórios de threat intelligence, threat actors e de incidentes de segurança

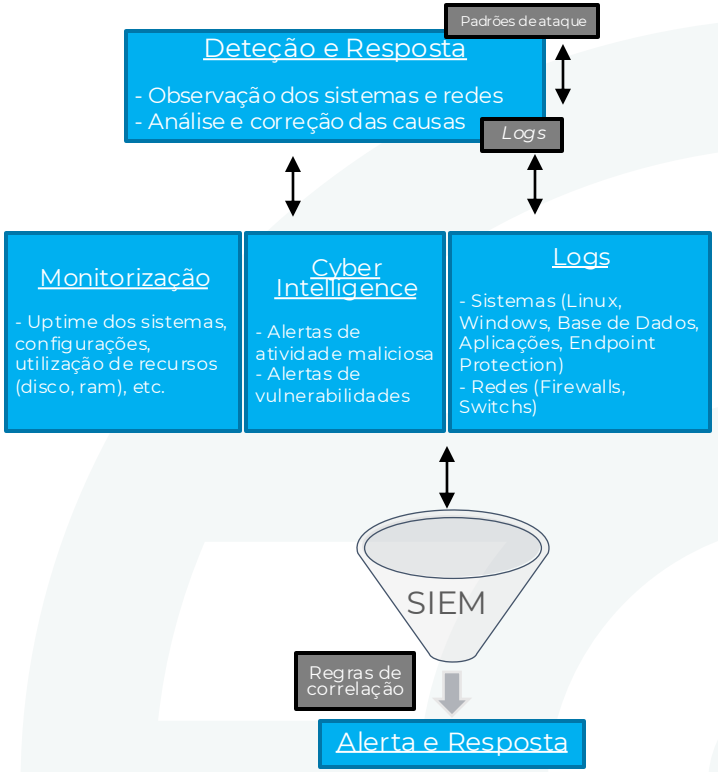
Plano de resposta a incidentes

Deteção

Desenvolver e implementar de medidas apropriadas para detetar eventos ou incidentes de segurança da informação. Atividades de monitorização de logs e alertas através do sistema SIEM são um exemplo.

Resposta

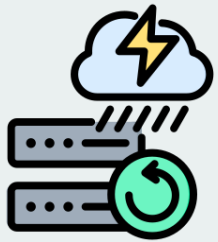
Desenvolver e implementar medidas apropriadas para agir quando detetado um incidente de cibersegurança. Neste contexto, são colocadas em prática as capacidades necessárias para conter como a definição de playbooks contra Ransomware.



Plano de resposta a incidentes

Recuperação

Desenvolver e implementar medidas apropriadas para manter planos de continuidade e de recuperação dos serviços críticos impactados por um incidente de cibersegurança, através do estabelecimento de um Plano de continuidade do negócio e de recuperação de desastre e de comunicação em crise.



Continuidade de Negócio

- Plano de continuidade e recuperação de desastres

Análise Forense

- Análise de logs e investigação

Continuidade de Negócio

Análise de Impacto no Negócio

Análise de Impacto nos Negócios é efetuada com recurso a questionários relativos à análise de impacto no negócio.

O processo é coordenado pelo Gestor da Continuidade de Negócio,

A análise de cada atividade é conduzida pela pessoa responsável em cada atividade.

A análise de Impacto no Negócios é realizada após a conclusão da Análise de Risco, de modo que as informações sobre os recursos necessários possam ser obtidas durante a análise de risco.

Análise de Impacto no Negócio

Questionario de Analise de Impacto de Negocio

Parte 1

1. Informação Geral acerca da actividade			
Nome da Organização		Nome da Pessoa Responsável	
Nome da atividade		E-mail:	
Morada		Data:	

2. Descrição da Actividade		
Descrição Breve da Actividade	Tarefas Chave e obrigações legais e contratuais:	Data Limite para execução

3. Impacto Geral de um Incidente Disruptivo (1- impacto marginal , 2 - impacto aceitavel , 3 - impacto alto, 4 - impacto catastrófico)						
	Descrição (se necessário)	2 horas	4 horas	24 horas	48 horas	1 semana
Perda de reputação da Organização:						
Reação dos Clientes						
Impacto de outras actividades na organização:						
Impacto na equipa de Saude e Segurança no Trabalho; Impactos Ambientais:						
Quanto difícil é recuperar o backlog:						

4. Impacto finaceiro do Incidente Disruptivo - Qual a perda Financeira causada pelo Incidente Disruptivo (em EUR)						
	Descrição se necessário	2 hours	4 hours	24 hours	48 hours	1 semana
Penalidades legais						
Penalidades Contratuais						
Perda de Receita de potênciais clientes:						
Perda de Receita de Clientes existentes:						
Despesas adicionais(reparações, manutenções, etc.)						

5. Comentários/ outra informação importante:

6. Conclusão (a ser preenchido pelo Gestor de Continuidade de Negocio)	
Maximo Periodo Tolerável de disrupção (Tempo Maximo de corte aceitavel)	

Análise de Impacto no Negócio

Questionário de Análise de Impacto no Negócio
Parte 2

7. Quantidade de trabalho	
Período (s) de maior volume de trabalho:	
Quantidade de trabalho executado durante períodos de maior volume de trabalho:	
Máxima quantidade de trabalho aceitável para a atividade imediatamente a seguir ao desastre:	
Período a partir do qual a quantidade normal de trabalho/nível de funcionamento deverá regularizar:	

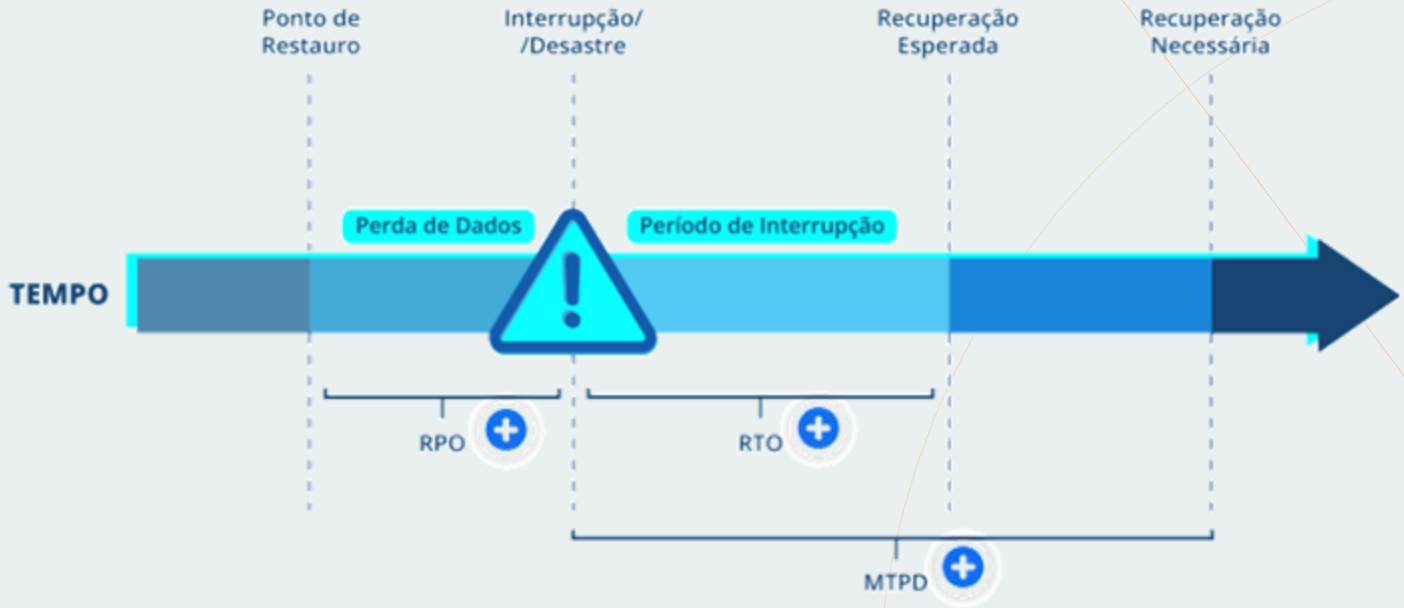
8. Recursos necessários para a recuperação										
				Tempo a partir do qual o recurso é necessário						
Nome do Recurso	Especificações	Quantidade	Ponto de Falha	Imediato	2 horas	4 horas	24 horas	48 horas	1 semana	Outro (especificar)
Pessoas:										
Aplicações e Base de dados:										
Dados guardados em formato electrónico (não incluído em aplicações e base de dados)										
Dados guardados em papel										
Equipamentos de IT e Comunicações										
Canais de Comunicação										
Outros equipamentos										
Infraestrutura e Instalações										
Capital necessário para a operação										
Serviços externos										

9. Dependencia de outros (Quem é necessário para a recuperação desta atividade)			
Dependência de outras actividades da equipa		Quais os documentos ou procedimentos que definem como é que a continuidade de negocio é assegurada por produtos ou serviços providenciados por parceiros, outsourcers e fornecedores em caso de disrupção de serviços:	Avaliação das capacidades da continuidade de negócio. (1 - inadequadas, 2 - algumas capacidades existem mas necessitam de melhorias, 3 - adequadas):
Dependencia de Parceiros ou Outsourcers:			
Dependencia de fornecedores			

10.Maximo de dados perdidos - quantidade de dados que podem ser perdidos (1 - impacto marginal, 2 - impacto aceitável, 3 - alto impacto, 4 - impacto catastrófico)						
	2 horas	4 horas	24 horas	48 horas	1 semana	São feitas copias de backup (sim/Não). Com que periodicidade
Aplicações e Base de dados:						
Dados guardados em formato electronico						
Dados guardados em papel						

11. Alternativas em caso de desastre	
Podem outras actividades sobreporem-se às operações desta actividade? Se sim, quais?	
Podem algumas das actividades ser desempenhadas manualmente, sem IT ou outro equipamento standard?	
12. Experiencia anterior	
Com que periodicidade incidentes disruptivos têm ocorrido até agora, e quanto tempo duraram?	
Como enfrentaram estas situações?	
13. Comentários/ outra informação importante	

Continuidade de Negócio



Continuidade de Negócio

Ameaças cibernéticas a um ccTLD

#1

Acesso não autorizado a informações

#2

Obtenção de credenciais

#3

Ransomware

#4

Registo de nomes de domínio fraudulentos

#5

Phishing/Smishing

Ameaças cibernéticas a um ccTLD

Acesso não autorizado a informações

Os cibercriminosos têm como objetivo exfiltrar informação pessoal dos titulares de domínios presentes nos sistemas de gestão de um ccTLD. Isto pode incluir:

- Nomes;
- Endereços de morada;
- Endereços de e-mail;
- Detalhes dos cartões de crédito;
- Dados de Negócio;

Ameaças cibernéticas a um ccTLD

Obtenção de Credenciais

Os cibercriminosos tentam adquirir credenciais de utilizadores internos de forma a obterem acesso ao sistema de gestão do ccTLD. As principais ameaças são:

- **Spear Phishing:** Ataques direcionados a funcionários através de emails falsos.
- **Ataques de brute-force:** Tentativas sistemáticas de adivinhar passwords.
- **Reutilização de passwords:** Aumenta o risco de comprometimento de contas.

Ameaças cibernéticas a um ccTLD

Ransomware

Os cibercriminosos podem encriptar a infraestrutura do registo de ccTLDs, exigindo um resgate para fornecer chaves de desencriptação. Isto pode causar interrupções significativas nos serviços prestados pelo registo de nomes de domínio dos ccTLDs.

Ameaças cibernéticas a um ccTLD

Registo de nomes de domínio fraudulentos

Os cibercriminosos criam versões falsas ou semelhantes de domínios existentes para se fazerem passar pelos domínios legítimos. Isso pode incluir a criação de websites maliciosos que imitam sites legítimos, frequentemente utilizados em ataques de phishing onde enganam os utilizadores a revelar informações sensíveis. Podem também vender estes domínios a terceiros que pretendem usá-los para atividades maliciosas.

Ameaças cibernéticas a um ccTLD

Phishing/Smishing

O Phishing é uma técnica comummente utilizada por cibercriminosos para obtenção de informações confidenciais sobre as pessoas (como nomes de utilizador e passwords).

EMAIL

SMS/WHATSAPP

CHAMADA TELEFÓNICA

DNS Abuse: O que é?

Conceito introduzido em 2021 com a revisão das Regras de Registo .pt. Nome de domínio utilizado, intencionalmente ou não, para a disseminação de **malware, phishing, pharming, botnets and/or spam**. (al. g) do Glossário das Regras de Registo).

É possível distinguir DNS abuse de duas formas:

- **Domínios registados com intenção maliciosa:** Domínio registado com a intenção de realizar atividades ilegais.
- **Domínios comprometidos:** Domínio registado para fins legítimos, mas comprometido por atores maliciosos para realizar atividades ilegais.

DNS Abuse: Atores

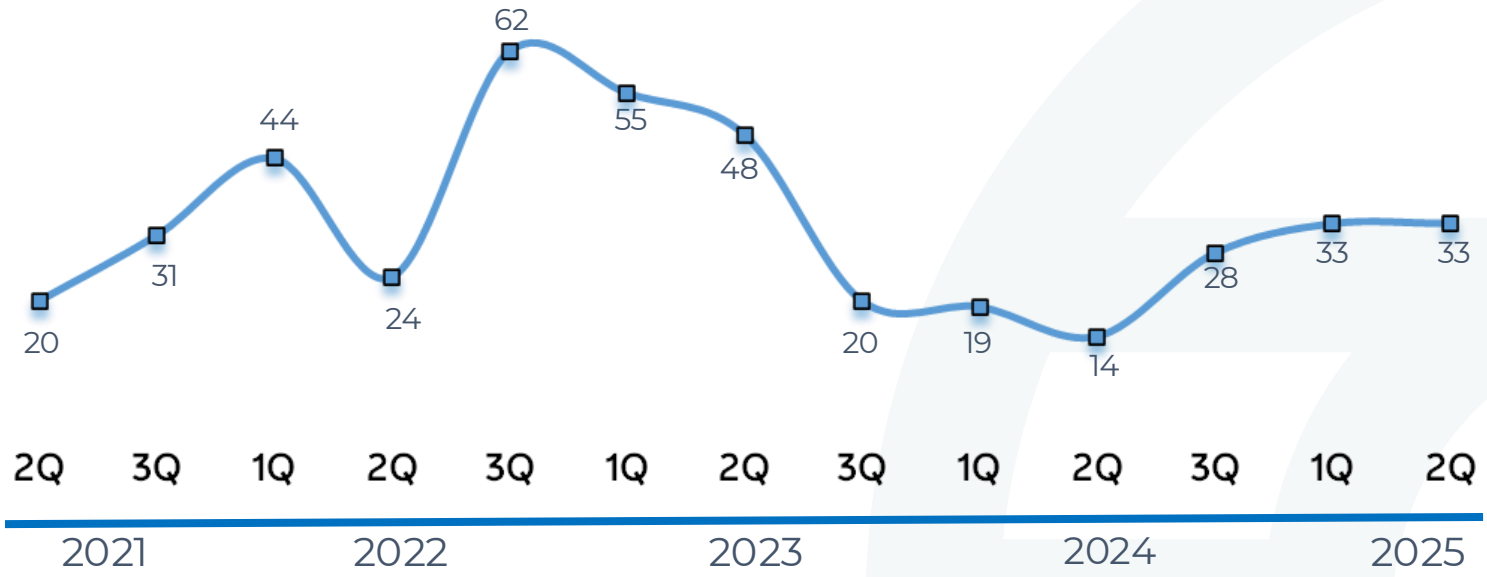
Atacante - O ator que regista o nome de domínio com intenções maliciosas ou que compromete um nome de domínio registado legitimamente (por exemplo, explorando websites vulneráveis).

Vítima - O utilizador da Internet e/ou terceiro afetado por atividades maliciosas realizadas através do nome de domínio registado, causando possível dano económico, reputacional ou físico.

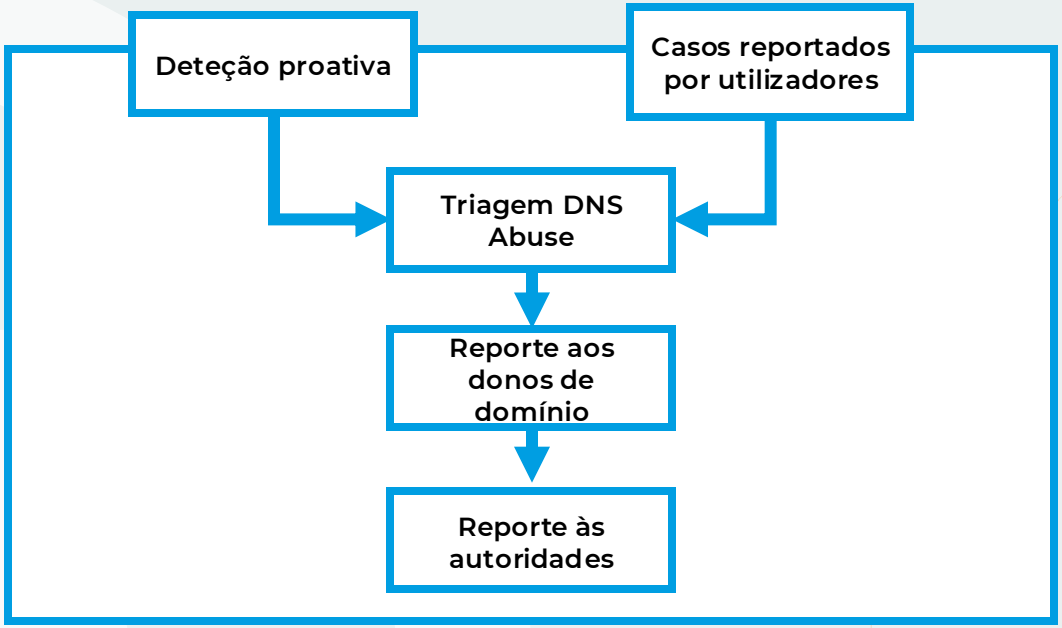
Intermediário - Principalmente operadores de serviços DNS (registries e registrars), ISPs, fornecedores de hosting ou outras plataformas online que facilitam a distribuição de conteúdo.

DNS Abuse: dados estatísticos

DNS Abuse	Phishing	Malware	Spam
431	356	67	8



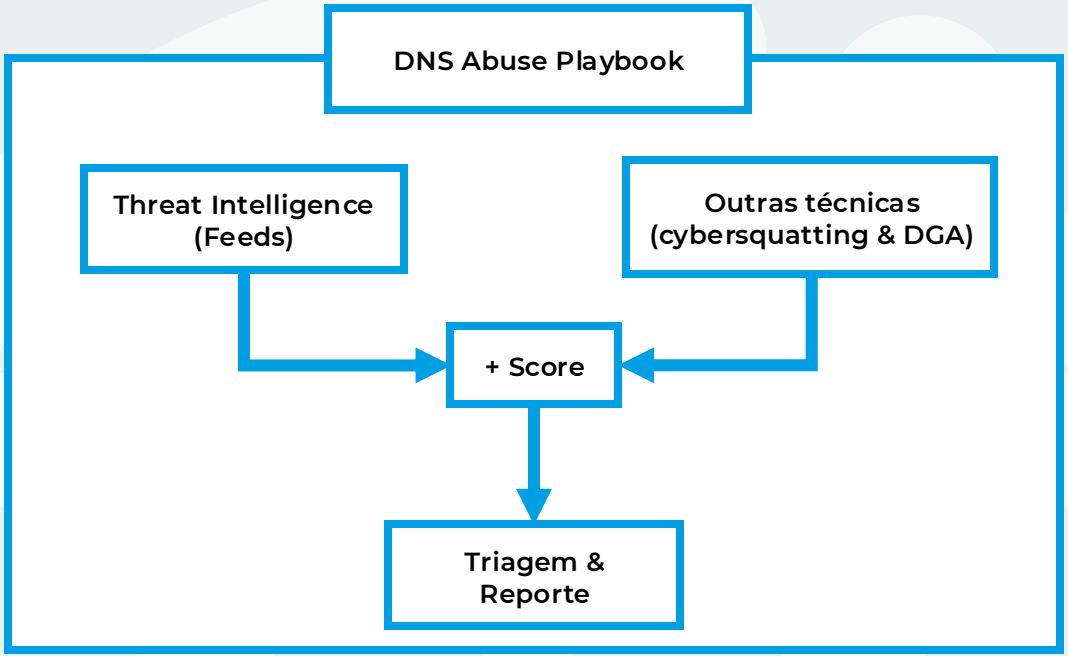
DNS Abuse: o que fazemos



Taxa de resolução à primeira tentativa

87.6%

DNS Abuse: o que fazemos



DNS Abuse: algumas técnicas

Typosquatting	whatsalpp.pt
Combosquatting	netflix-payments.pt
Bitsquatting	micposoft.pt
Doppelganger Squatting	wwwgoogle.pt

DNS Abuse: algumas técnicas

Homographsquatting	microsoft.pt
Levelsquatting	microsoft.com.2xmpq.pt
Soundsquatting	4ever21.pt

DGA: Domain Generated Algorithm

DGA, Domain generated algorithm

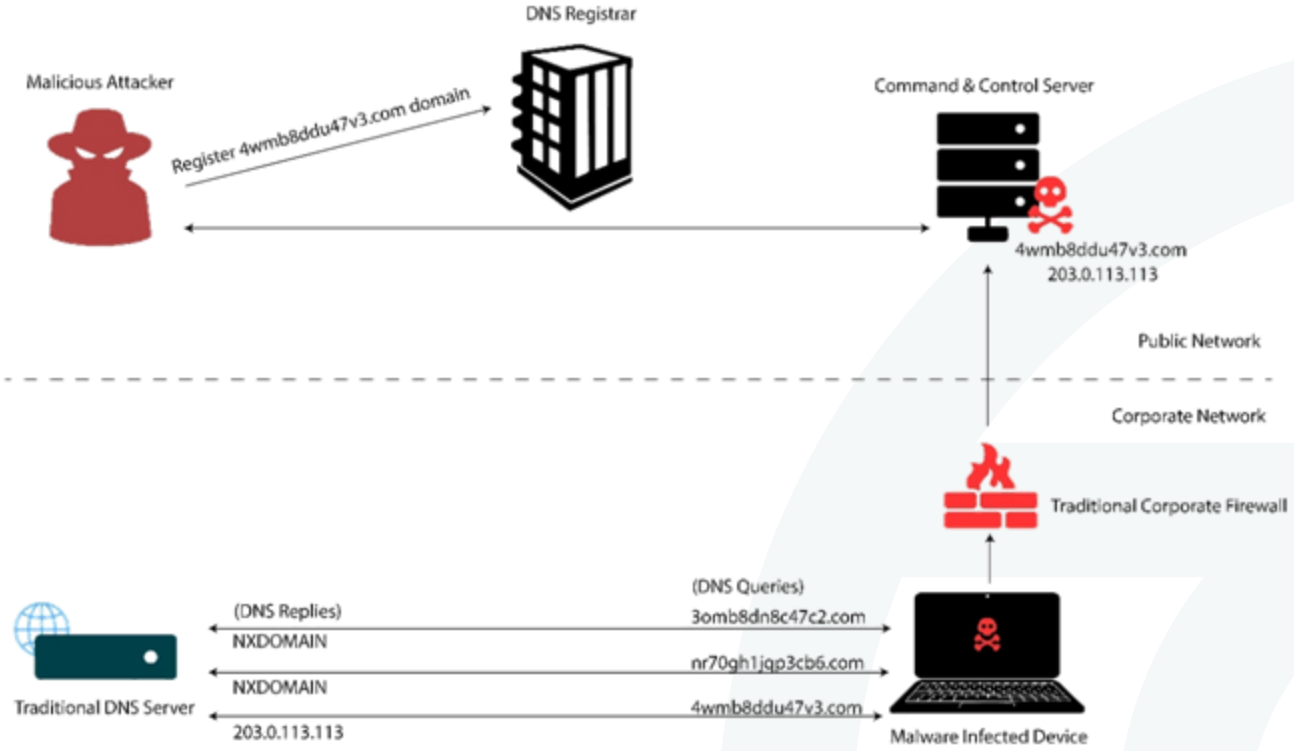
Tradicionalmente, o malware usava domínios ou endereços IP codificados para C&C.

- Com técnicas de engenharia reversa, é possível identificar o binário do malware e colocar na lista negra
- É fácil retirar ou colocar na lista negra os domínios ou endereços IP utilizados.

Utilizando técnicas DGA, os nomes de domínio são gerados com base numa semente aleatória e num algoritmo (dependente da família de malware).

- Não há domínios para identificar com engenharia reversa
- Não é possível parar o C&C do malware.

DGA: Domain Generated Algorithm



Source: https://www.tcpwave.com/WHITE-PAPERS/DGA-for-Web.html

DNS Abuse: técnicas de deteção

O nome de domínio contém palavras suspeitas.

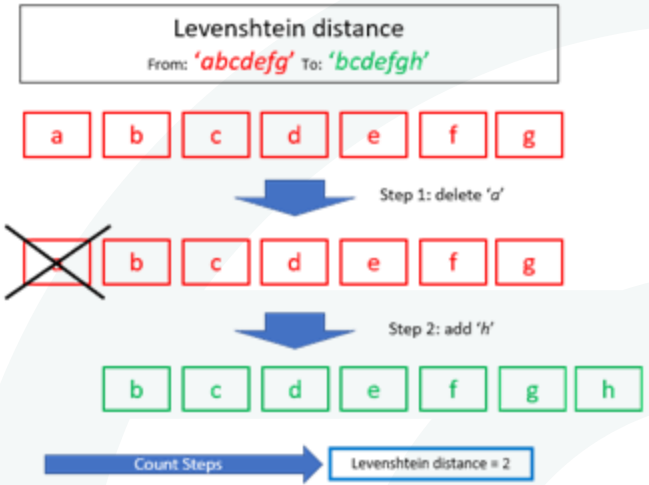
- Avaliar a presença de uma palavra comumente relacionada com atividade maliciosa

  Por exemplo: **googleee**.pt contém a palavra "**google**".

O nome de domínio é semelhante a um conjunto de nomes monitorizado.

- Avaliar a distância do nome de domínio a palavras comumente relacionadas com atividade maliciosa, com base no método de distância de Levenshtein.

  Por exemplo: **googl3**.pt está à distância de 1 letra "**google**".



DNS Abuse: técnicas de deteção

O nome de domínio utiliza caracteres IDN semelhantes ou outros caracteres "confusos".

- Avaliar a presença de caracteres "confusos" dentro do nome de domínio.

  Por exemplo: Paypal.pt é diferente de “Paypa**l**.pt”.

O nome de domínio apresenta um alto grau de aleatoriedade devido à variedade de letras, números e símbolos (relacionados com DGA).

- Avaliar a probabilidade do domínio estar associado a C&C, com base no método de entropia de Shannon.

$$H = -\sum p(x)\log p(x)$$

Por exemplo:

pt.pt – Entropia 1.0 (Muito Baixo)
google.pt – Entropia 1.9 (Muito Baixo)
ppjnwgxe2bmc3mi95wu6hbbc.pt – Entropia 4.0 (Muito Alto)

DNS Abuse: o que podemos fazer

Melhorar a segurança do meu domínio

- Protocolo HTTPS;
- Protocolo DNSSEC;
- Protocolos de e-mail (SPF, DKIM e DMARC);

DNS Abuse: o que podemos fazer

Protocolo HTTPS

HTTPS (Hypertext Transfer Protocol Secure) é um protocolo que permite estabelecer uma ligação segura entre o browser do utilizador e o servidor de um site. Este protocolo proporciona:

- **Confidencialidade:** Os dados são encriptados em trânsito.
- **Integridade:** Uma vez que a integridade dos dados é verificada, estes não podem ser adulterados durante a sua transmissão

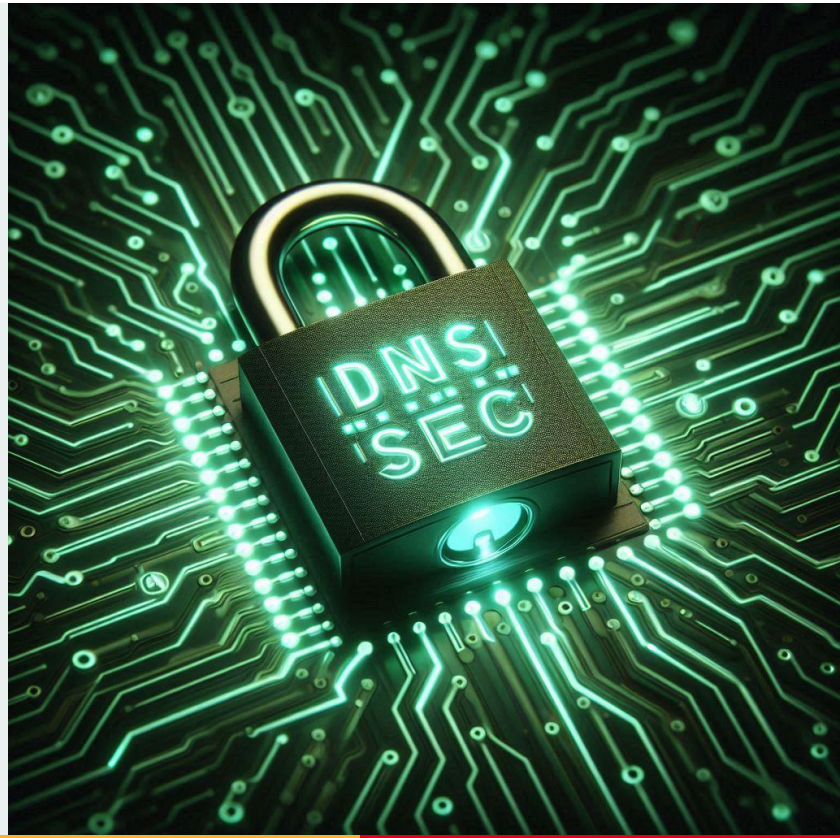
DNS Abuse: o que podemos fazer

Protocolo DNSSEC

O DNSSEC é um conjunto de extensões de segurança para o DNS (Sistema de Nomes de Domínio). Funciona como uma assinatura digital para os dados do DNS, garantindo que as informações que são recebidas pelo utilizador, sobre um site, são autenticas e não foram alteradas por terceiros.

Assenta no seguintes 3 principios:

- **Autenticidade** – A origem da informação DNS é a suposta;
- **Integridade** – A informação DNS não é alterada em trânsito, desde que foi assinada na origem;
- **Proof of Non-Existence** – Resposta autenticada da não existência de um domínio.

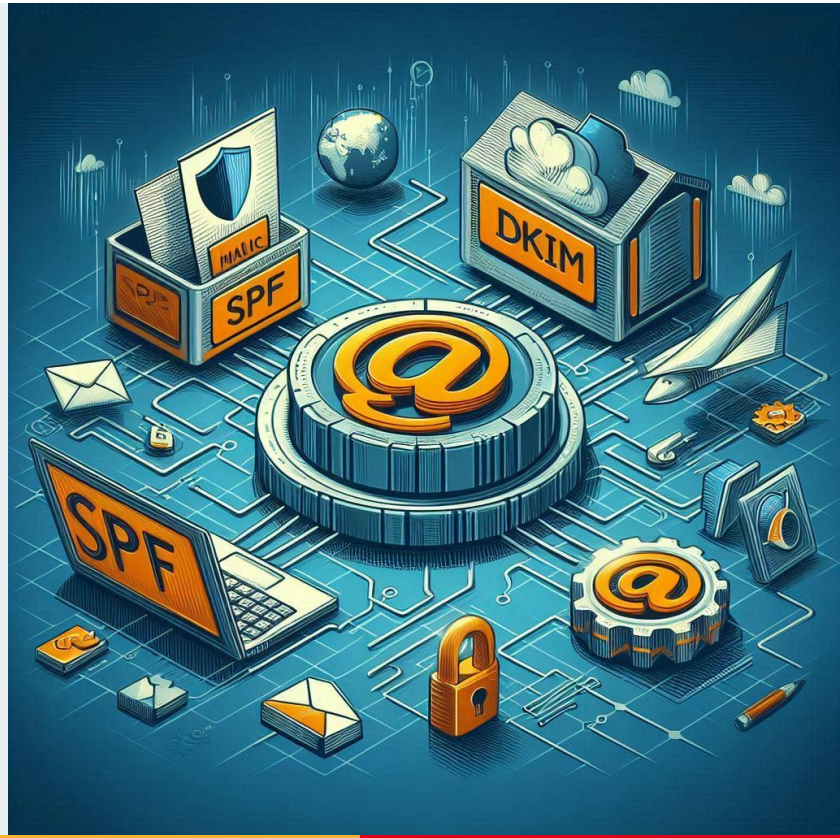


DNS Abuse: o que podemos fazer

Protocolos SPF, DKIM e DMARC

O SPF, DKIM e DMARC são protocolos de segurança que trabalham em conjunto para autenticar a origem dos emails.

- **SPF (Sender Policy Framework):** Define quais servidores são autorizados a enviar emails em nome de um domínio;
- **DKIM (DomainKeys Identified Mail):** Adiciona uma assinatura digital aos emails, provando que a mensagem não foi alterada durante o trajeto;
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Define as políticas para os emails que não passam nos testes de SPF e DKIM.



Protocolos de Segurança na zona .pt

Maturidade de implementação de protocolos de segurança no .pt

Projeto desenvolvido no âmbito de uma dissertação de mestrado, com os objetivos:

- Desenvolver solução automatizada de análise do nível de adoção de protocolos de segurança dos domínios ativos na zona .pt,
- Catalogar os resultados por setores de atividades e identifica as barreiras à sua implementação e propor estratégias para aumentar a implementação dos mesmos.

1. Ferramenta Automatizada

Desenvolvida em Python para analisar o estado da implementação dos protocolos de segurança (SPF, DKIM e DMARC) em domínios .pt;

2. Recolha de Dados

Recolha de dados diretamente dos registos DNS dos domínios através de métodos de crawling DNS;

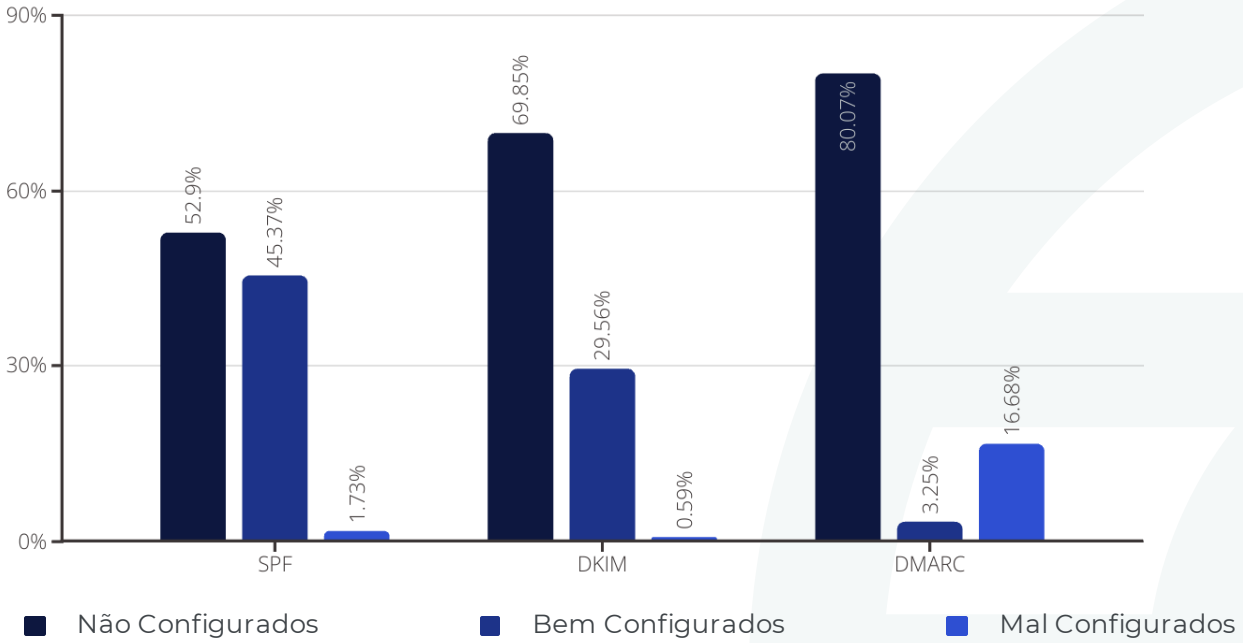
3. Classificação Automática dos Domínios

A ferramenta avalia automaticamente cada domínio .pt, classificando em três categorias:

- Bem configurado
- Mal configurado
- Não configurado

Scans da Zona

Taxa de implementação de protocolos de segurança no email



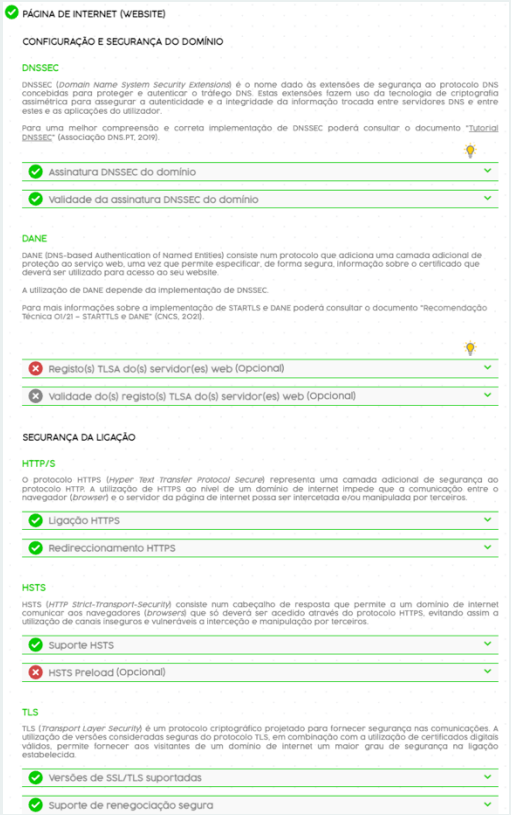
DNS Abuse: o que podemos fazer

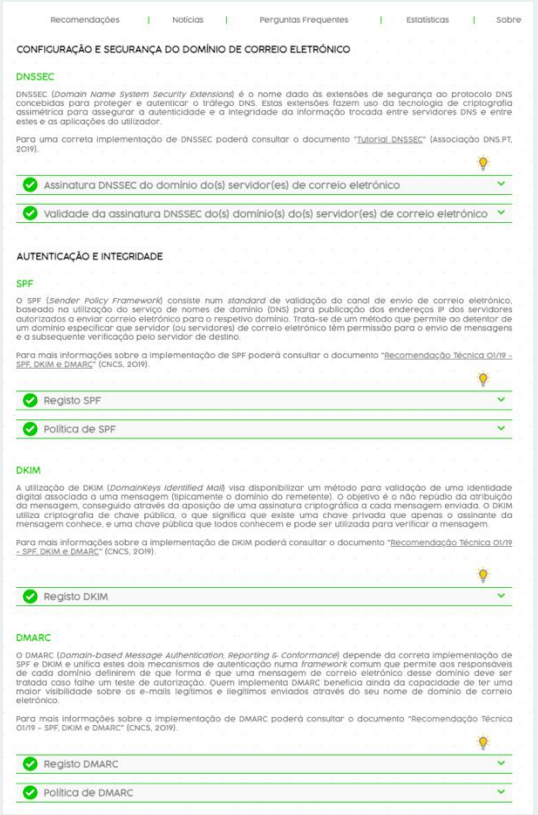
Webcheck

A Webcheck.pt é uma iniciativa conjunta do Centro Nacional de Cibersegurança (CNCS) e da Associação DNS.PT (.PT) que tem como objetivo promover a adoção de boas práticas e standards que contribuam para garantir a segurança, integridade e confidencialidade nas comunicações através da internet.

DNS Abuse: o que podemos fazer

Webcheck





Formação PTSOC

Como parte da nossa missão realizamos regularmente workshops e ações de sensibilização nas diferentes matérias de cibersegurança.

Gestão dos Riscos de Cibersegurança nas Organizações

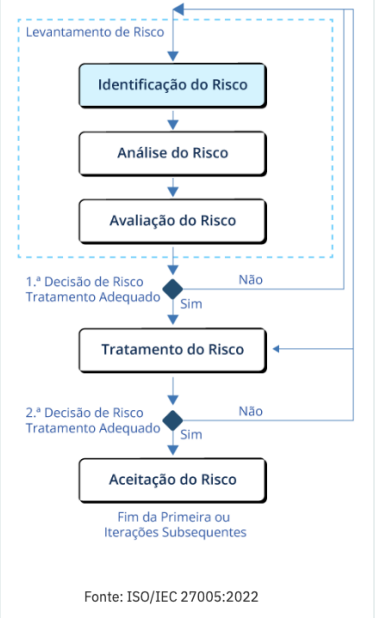
Cód. GRCO

Salvaguarde a integridade da sua organização identificando vulnerabilidades e planeando estratégias de mitigação em caso de ciberataque.

Duração: 10 horas Esforço: 10 horas Ritmo: Ao ritmo do estudante

Idiomas: Português

8.825 já inscritos!



Fonte: ISO/IEC 27005:2022

Formação PTSOC

Como parte da nossa missão realizamos regularmente workshops e ações de sensibilização nas diferentes matérias de cibersegurança.

Gestão da Continuidade de Negócio

Cód. CNCIS

O que deve uma organização fazer quando um evento interrompe a normal entrega de bens ou serviços? Inscreva-se neste curso para aprender os princípios básicos de gestão da continuidade de negócio.

Duração: 10 horas Esforço: 10 horas Ritmo: Ao ritmo do estudante

Idiomas: Português

3.940 já inscritos!

- 0. Boas-Vindas
- 1. Introdução à Continuidade de Negócio
- 2. Análise de Impacto no Negócio e do Risco
  - Introdução ao Módulo
  - 2.1. Análise de Impacto no Negócio
  - 2.2. Gestão dos Riscos
  - Avaliação do Módulo (5 Questions)
    Avaliação Final do Módulo
- 3. Plano de Continuidade de Negócio
  - Introdução ao Módulo
  - 3.1. Estratégias de Continuidade de Negócio
  - 3.2. Planos de Continuidade de Negócio
  - Avaliação do Módulo (5 Questions)
    Avaliação Final do Módulo
- 4. Governo, Exercícios, Formação e Revisão
- 5. Caso Prático
- Fim do Curso

Questões?

Mais informações no nosso website ptsoc.pt

Contactos: ptsoc@pt.pt

LusNIC
Associação de ccTLDs de língua portuguesa

Coalition for Digital Africa

ICANN

OBRIGADO!

lusnic@lusnic.org