

Portugal

Sol, Mar e Vulnerabilidades

CDAYS - 2024

\$whoami

- ▶ Pedro Vieira
- ▶ Engenheiro de Cibersegurança
- ▶ Certified Ethical Hacker
- ▶ Licenciado pela Universidade do Minho



Aviso Legal & Leis

Aviso Legal

Disclaimer - Aborrecido, mas necessário

- ▶ Toda a informação contida nesta apresentação destina-se exclusivamente para **fins educacionais e de consciencialização**.
- ▶ **Apresentação ao vivo**. Não é um ambiente controlado e alguns conteúdos podem ser inapropriados para alguns participantes.
- ▶ **Declino qualquer responsabilidade** pelo uso, uso indevido, download, ou visualização dos links desta apresentação.
- ▶ Esta apresentação **não está diretamente relacionada** com o meu trabalho ou empregador.



Aviso Legal

Disclaimer - Evitem atividades ilegais

- ▶ Alguns links, sites, software ou outros itens listados podem ou não ser legais, delito, crime no seu país.
- ▶ Por favor, **verifique que lhe é permitida** a consulta dos sites, e o eventual uso do software listado.
- ▶ Ignorância acerca das leis aplicáveis **não é desculpa** para transgressões ou actividades ilegais.
- ▶ Atividades ilegais podem implicar problemas ou mesmo prisão.
- ▶ **Verifique sempre o que é legal e as leis aplicáveis.**



Leis

Lei Portuguesa e Organizações

► Lei

- Diário República Eletrónico ([link](#)) ➡
- ANACOM ([link](#)) ➡

► Organizações

- CNCS – Centro Nacional de Cibersegurança ([link](#)) ➡
 - Notificação de Incidentes ([link](#)) ➡
 - CERT.PT ([link](#)) ➡
- Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) ([link](#)) ➡
- Ministério Público ([link](#)) ➡

Agenda

- Vulnerabilidade
- Vetores de Ataque Comuns
- Paisagem Portuguesa

Vulnerabilidade

Definição e Estatísticas

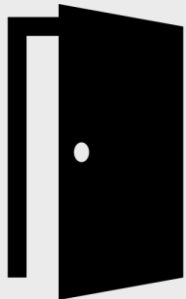

Vulnerabilidade

Vulnerabilidade vs Incidente

Vulnerabilidade

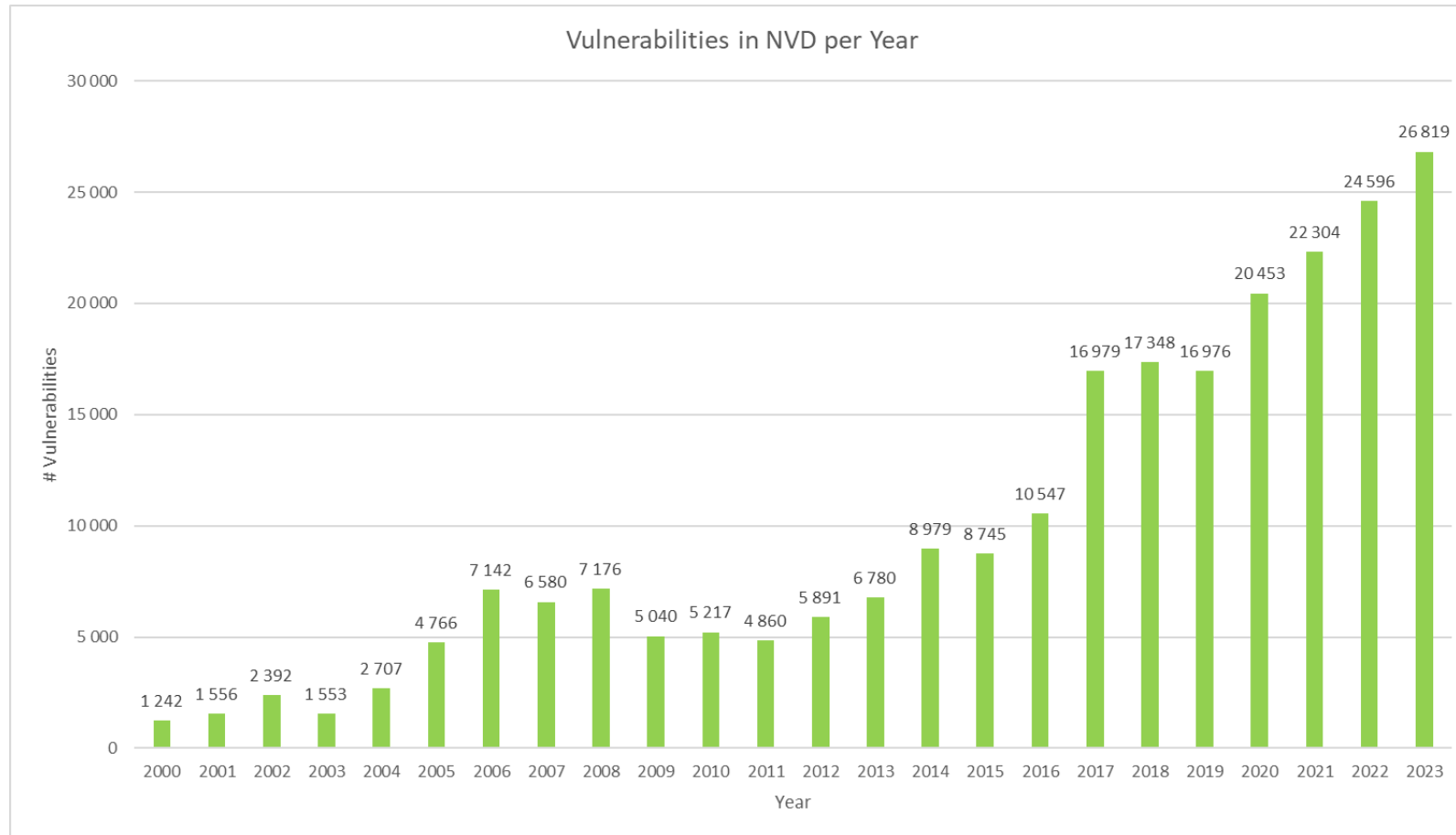
"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to **confidentiality, integrity, or availability.**"

National Vulnerability Database - <https://nvd.nist.gov/vuln>

Vulnerabilidade	Incidente
Porta aberta 	Acesso não autorizado 

Vulnerabilidade

Estatísticas por Ano



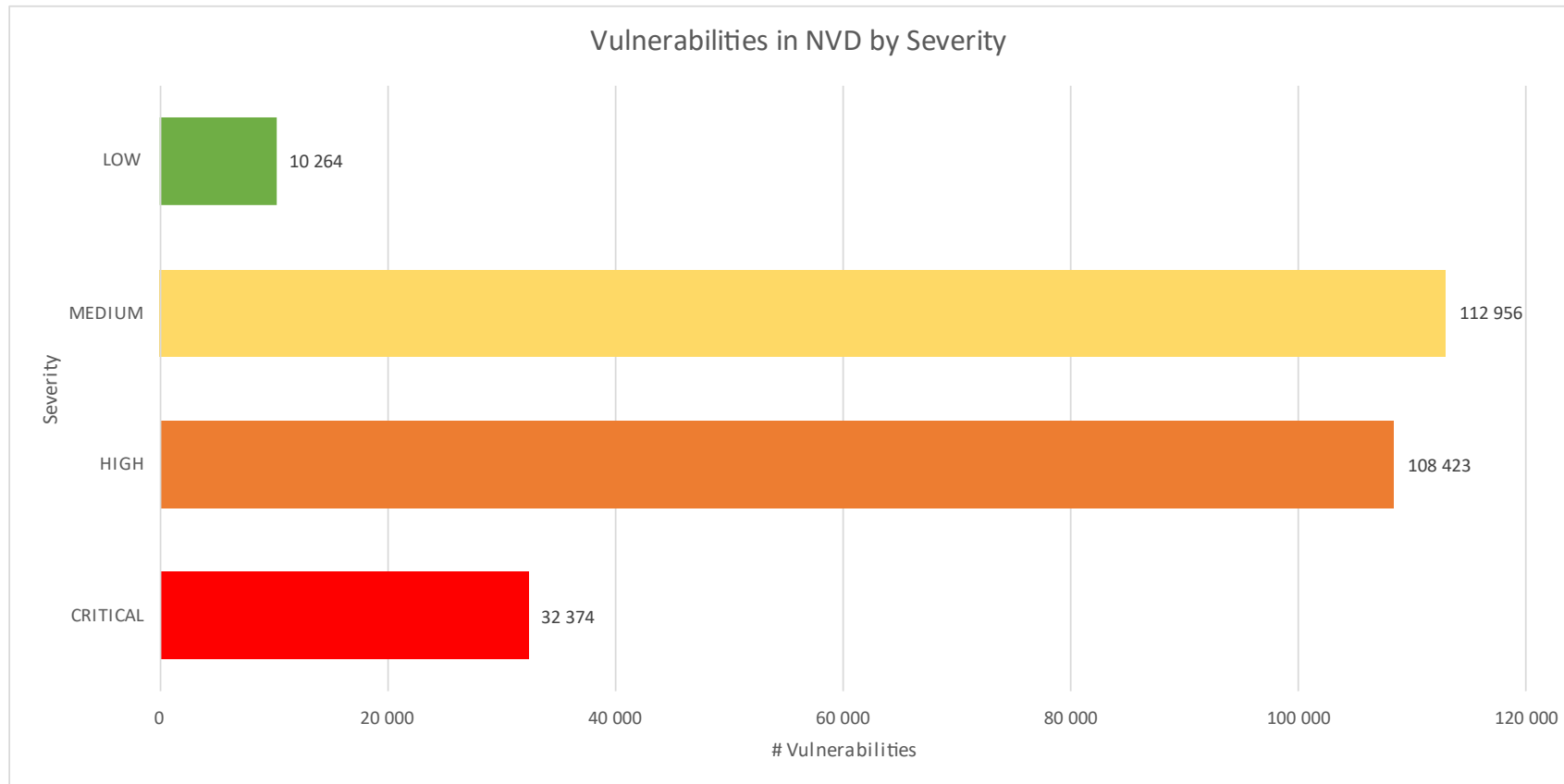
Total de
vulnerabilidades
conhecidas

283.154

Source NVD 14/03/2024

Vulnerabilidade

Estatísticas por Gravidade



CVSS v3.1 Ratings	
LOW	0.1 - 3.9
MEDIUM	4.0 - 6.9
HIGH	7.0 - 8.9
CRITICAL	9.0 - 10.0

Source NVD 14/03/2024

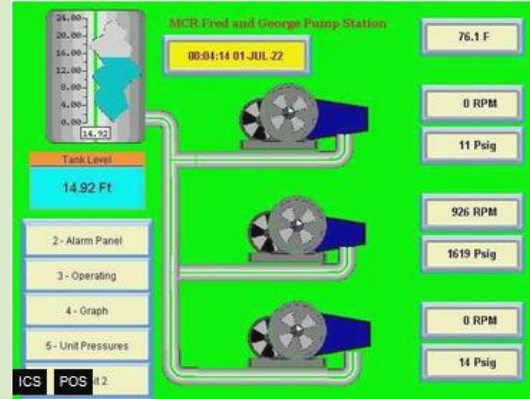
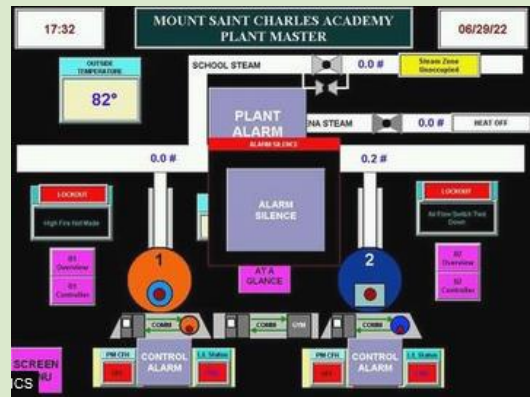
Vulnerabilidade

Exemplos do Shodan.io

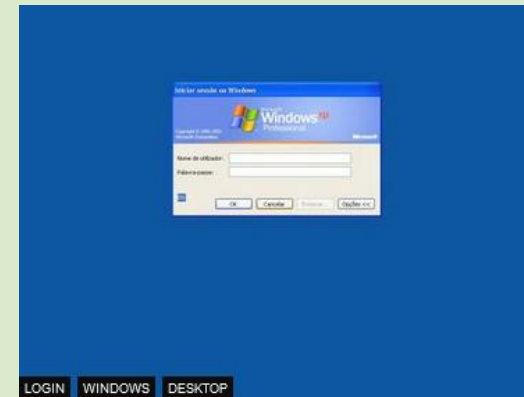
Default/Sem Password



Sistemas Controlo Industrial



Sistemas Vulneráveis



Vetores de Ataque Comuns

Easy-Peasy

Vetores de Ataque Comuns

Credenciais

Inseguras	Comprometidas/Expostas
<ul style="list-style-type: none">Sem passwordDefault credentials (admin/admin)Passwords fracasPasswords reutilizadas	<ul style="list-style-type: none">Sites legítimos hackeados vazam informação de utilizadores e credenciaisMother of all breaches reveals 26 billion records

Vetores de Ataque Comuns

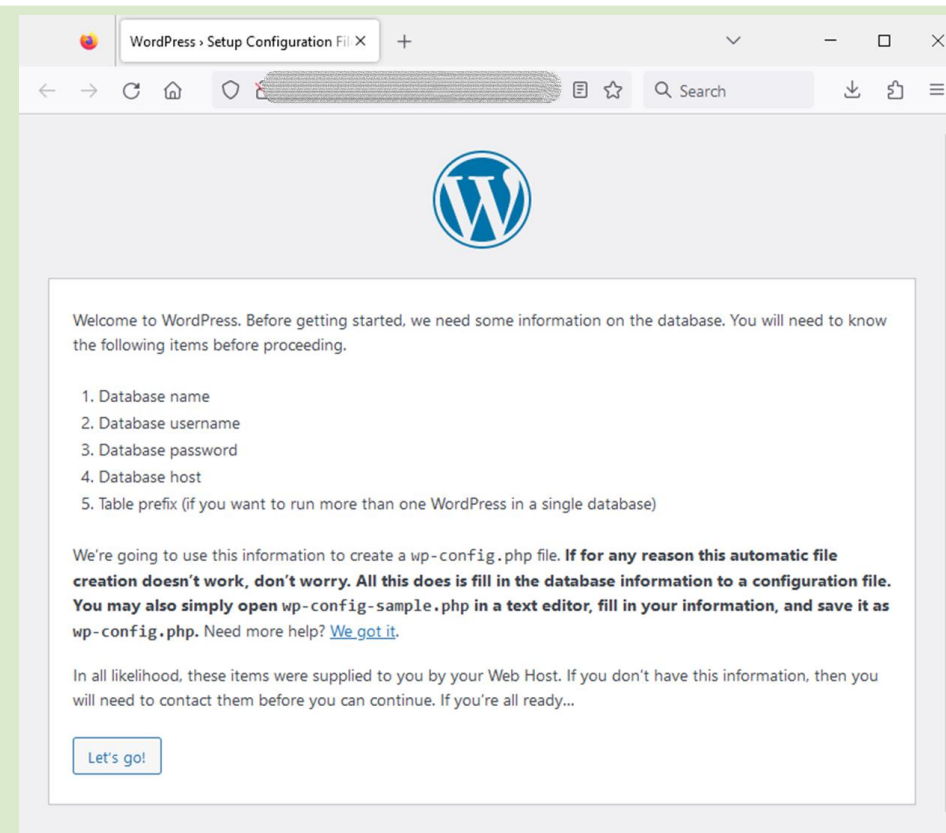
Erros de configuração

Pastas Partilhadas - Autenticação desabilitada

SMB Status: Authentication: disabled SMB Version: 2 Capabilities: raw-mode		SMB Status: Authentication: disabled SMB Version: 2 Capabilities: raw-mode		SMB Status: Authentication: disabled SMB Version: 2 Capabilities: raw-mode	
Shares		Shares		Shares	
Name	Type	Name	Type	Name	Type

projetos	Disk	Programas	Disk	Multimedia	Disk
arquivo	Disk	FINANCEIRO	Disk	Download	Disk
administrativo	Disk	ADMINISTRATIVO	Disk	Web	Disk
software	Disk	COMERCIAL	Disk	Public	Disk
contabilidade	Disk	CONTABILIDADE	Disk	homes	Disk
pec-cladmara	Disk	FATURAMENTO	Disk	Projetos	Disk
pec-helio	Disk	FERNANDO	Disk	GuardDB	Disk
pec-augusto	Disk	LABORATORIO	Disk	GuardRecording	Disk
pec-sergio	Disk	LOGISTICA	Disk	GuardAutoSnap	Disk
pec-antunes	Disk	MARCOS	Disk	Contabilidade	Disk
pec-fabiane	Disk	RH	Disk	Admin	Disk
pec-eng1	Disk	Public	Disk	Container	Disk
pec-eng2	Disk	print\$	Disk	Browser Station	Disk
pec-eng3	Disk	IPC\$	IPC	QmailAgent	Disk
pec-eng4	Disk			Madalena	Disk
print\$	Disk			Sara	Disk
IPC\$	IPC			Ines	Disk
				HTProjetos	Disk
				PAG	Disk
				home	Disk
				IPC\$	IPC

WordPress site - Configuração acessível



Vetores de Ataque Comuns

Vulnerabilidades em Software

Pastas Partilhadas - Execução Remota de Código

Vulnerabilities

CVE-2020-0796 **10.0** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.11 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client.

SMB Status:

Authentication: disabled
SMB Version: 2
Capabilities: raw-mode

Shares

Name	Type	Comments
ADMIN\$	Disk	Admin remoto
C\$	Disk	Partilha predefinida
credTec	Disk	
D\$	Disk	Partilha predefinida
Executavel	Disk	
IPC\$	IPC	IPC remoto
passagem	Disk	
PHCSistema	Disk	
Users	Disk	
validacc	Disk	

Website - Múltiplas vulnerabilidades

PLANO NACIONAL
DE FORMAÇÃO FINANCEIRA

TODOS CONIAM


PLANEAR O
ORÇAMENTO
FAMILIAR

FAZER
PAGAMENTOS

POUPAR E
INVESTIR



 **ETAPAS DA VIDA**

 **ESTUDAR**

 **COMEÇAR A TRABALHAR**

 **COMPRAR CARRO**

 **COMPRAR CASA**

 **CONSTITUIR FAMÍLIA**

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-45802

5.9 When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that. This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During 'normal' HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVE-2023-31122

7.5 Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server. This issue affects Apache HTTP Server: through 2.4.57.

CVE-2023-25690

9.8 Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine On RewriteRule ^/here/^(.*) "http://example.com:8080/elsewhere?\${1}" [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

CVE-2022-37436

5.3 Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVE-2022-36760

9.0 Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

Vetores de Ataque Comuns

Malware - Ransomware

Redeemer Ransomware

Redeemer Ransomware - Your Data Is Encrypted

8888888b. 888
888 Y88b 888
888 888 888
888 d88P.d88b. .d88888 .d88b. .d88b. 88888b.d88b. .d88b. 888d888
88888888P" d8P Y8b d88" 888 d8P Y8b d8P Y8b 888 "888 "88b d8P Y8b 888P"
888 T88b 88888888 888 888 88888888 88888888 888 888 888888888 888
888 T88b Y8b. Y88b 888 Y8b. Y8b. 888 888 888 Y8b. 888
888 T88b "Y8888 "Y8888 "Y8888 "Y8888 888 888 888 "Y8888 888

Made by Cerebrate
Visit the official Redeemer Ransomware Tor website -
redeemergd6jtzgiuf5jgpkk6i3xybkhsldzjoyjaxivyZlnhvmzcad.onion

[Question 1] What happened to my computer?
I cannot access my files and they have changed their extension?
[Answer 1] Your files have been encrypted by Redeemer, a Darknet ransomware operation.

[Question 2] Is there any way to recover my files?
[Answer 2] Yes, you can recover your files. This will however cost you money in Monero (XMR).

[Question 3] Is there any way to recover my files without paying?
[Answer 3] Without paying for the proper decryption key, you will NEVER regain access to your files.
Redeemer uses the most secure algorithms and a sophisticated encryption scheme which guarantees security.
Ever since Redeemer was first released publicly (~May 2021) no one managed to crack the decryption or recover their files without paying.

OK

Ransomwatch

summary

may 4th, 2024

ransomwatch is currently crawling 382 sites belonging to 192 unique groups

⌚ there have been 31 posts within the last 24 hours

📅 there have been 64 posts within the month of may

📅 there have been 1286 posts within the last 90 days

📅 there have been 1712 posts within the year of 2024

🔍 there are currently 100 online hosts & 120 custom parsers.

🕒 ransomwatch has been running for 2 years, 7 months and 28 days and indexed 11169 posts

all data ([groups](#)) and ([posts](#)) is available in JSON (updated hourly)

ransomwatch is fully [open source](#). please consider [sponsoring](#) if you find it useful!

Vetores de Ataque Comuns

Malware - Ransomware

Ransomwatch

recent posts

last 200 posts

date	title	group
2024-05-04	firstmac.com.au	embargo
2024-05-04	mulfordconstruction.com	embargo
2024-05-04	bulldogbag.com	underground
2024-05-04	frenckengroup.com	underground
2024-05-04	synology.com	underground
2024-05-04	tpa-group.sk	underground
2024-05-04	Triathlon.group	underground
2024-05-04	awwg.com	underground
2024-05-04	kc.co.kr	underground
2024-05-04	Y. Hata & Co., Ltd.	underground
2024-05-04	Skender Construction	underground
2024-05-04	Creative Business Interiors	underground
2024-05-04	cochraneglobal.com	underground
2024-05-04	ikfhomefinance.com	darkvault
2024-05-04	The Islamic Emirat of Afghanistan National Environmental Protection Agency <nepa.gov.af/df	ransomhub
2024-05-04	Accounting Professionals LLC. Price, Breazeale & #838; Chastang	everest
2024-05-04	Bitfinex	flocker
2024-05-04	SBC Global	flocker
2024-05-04	Rutgers University	flocker
2024-05-04	Coinmoma	flocker

NoMoreRansom

<🔒/> NO MORE RANSOM

NEED HELP
unlocking your digital
life without paying
your attackers*?

YES

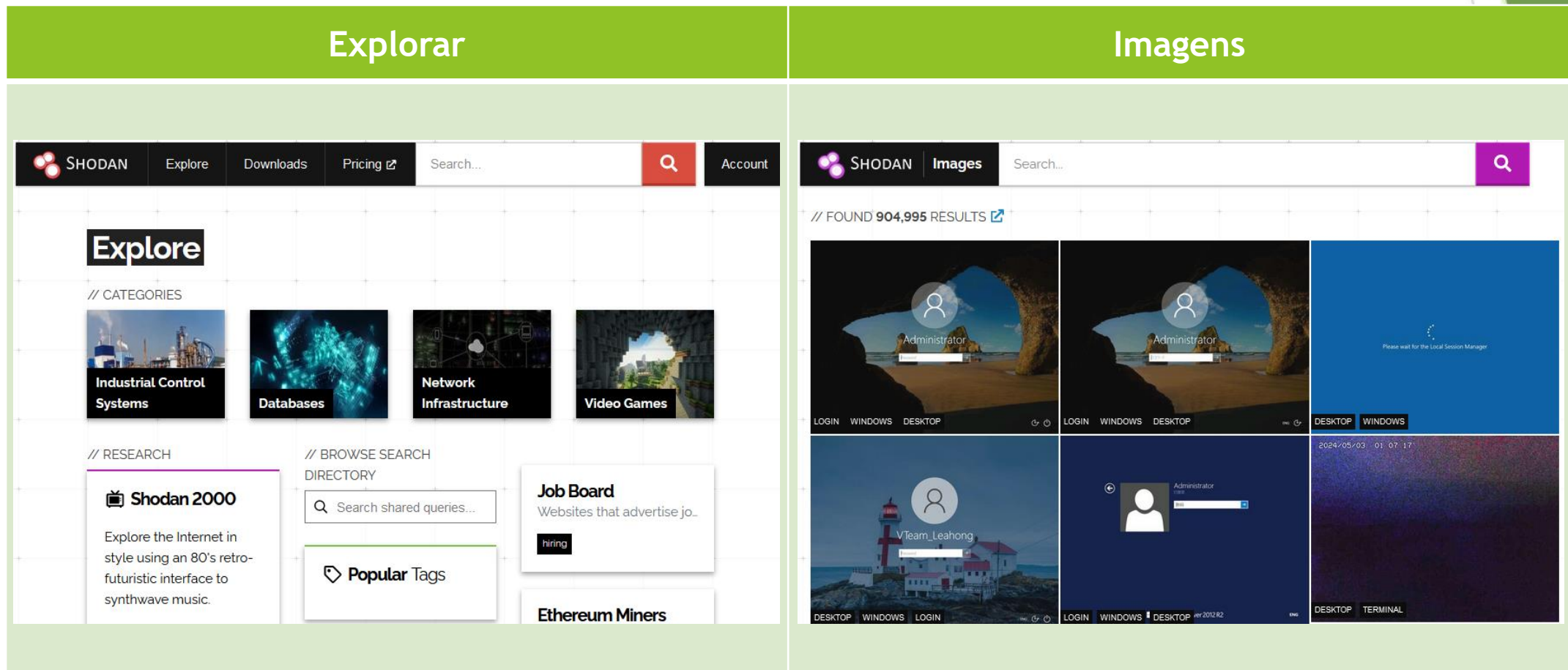
NO

At the moment, not every type of ransomware has a solution. Keep checking this website as new keys and applications are added when available.

Paisagem Portuguesa

Portugal

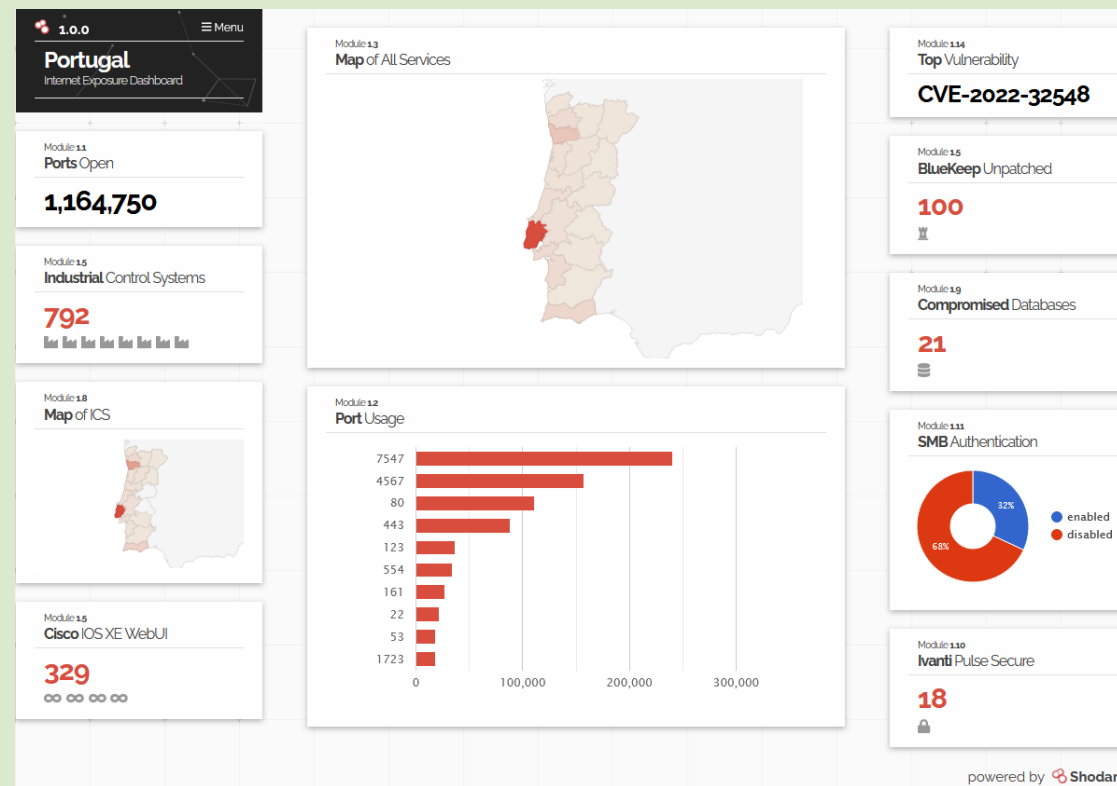
Shodan.io - Motor de busca - Internet Of Things



Portugal



Shodan.io - Motor de busca - Internet Of Things

Internet Exposure Observatory



Portugal

Shodan.io - Motor de busca - Internet Of Things

Top in Portugal - CVE-2022-32548	EternalBlue - MS17-010 - CVE-2017-0144																								
<div> Vulnerabilities</div> <div>CVE-2022-32548 10.0 Unauthenticated Remote Code Execution in a Wide Range of DrayTek Vigor Routers</div>	<div> Vulnerabilities</div> <div>MS17-010 8.1 This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server. This security update is rated Critical for all supported releases of Microsoft Windows.</div>																								
<div>TOTAL RESULTS</div> <div>3,322</div>	<div>TOTAL RESULTS</div> <div>6</div>																								
<div>TOP CITIES</div> <table><tr><td>Lisbon</td><td>991</td></tr><tr><td>Leiria</td><td>181</td></tr><tr><td>Porto</td><td>114</td></tr><tr><td>Braga</td><td>95</td></tr><tr><td>Rio Maior</td><td>83</td></tr><tr><td>More...</td><td></td></tr></table>	Lisbon	991	Leiria	181	Porto	114	Braga	95	Rio Maior	83	More...		<div>TOP CITIES</div> <table><tr><td>Lisbon</td><td>2</td></tr><tr><td>Braga</td><td>1</td></tr><tr><td>Porto</td><td>1</td></tr><tr><td>Silves</td><td>1</td></tr><tr><td>Évora</td><td>1</td></tr><tr><td>More...</td><td></td></tr></table>	Lisbon	2	Braga	1	Porto	1	Silves	1	Évora	1	More...	
Lisbon	991																								
Leiria	181																								
Porto	114																								
Braga	95																								
Rio Maior	83																								
More...																									
Lisbon	2																								
Braga	1																								
Porto	1																								
Silves	1																								
Évora	1																								
More...																									

Portugal

Shodan.io - Motor de busca - Internet Of Things

Heartbleed - CVE-2014-0160

⚠ Vulnerabilities

CVE-2014-0160 **5.0** The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

TOTAL RESULTS

311

TOP CITIES

Lisbon	146
Coimbra	20
Porto	12
Rio Maior	8
Torres Vedras	7

[More...](#)

SMBGhost - CVE-2020-0796

⚠ Vulnerabilities

CVE-2020-0796 **10.0** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.11 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client.

TOTAL RESULTS

554

TOP CITIES

Lisbon	263
Porto	29
Braga	13
Guimarães	8
Montijo	8

[More...](#)

Portugal

Shodan.io - Motor de busca - Internet Of Things

BlueKeep - CVE-2019-0708

Vulnerabilities

CVE-2019-0708 10.0 A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

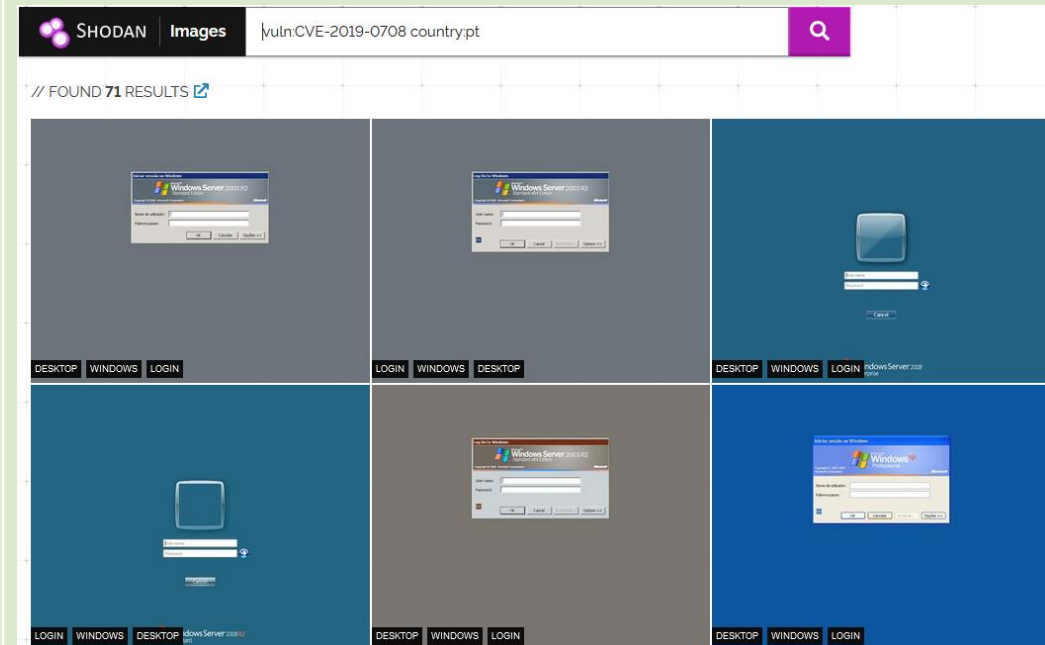
TOTAL RESULTS

99

TOP CITIES

Lisbon	30
Porto	11
Braga	5
Leiria	3
Espinho	2

[More...](#)



Portugal

Shodan.io - Motor de busca - Internet Of Things

Pastas Partilhadas

TOTAL RESULTS

4,261

TOP CITIES

Lisbon	518
Porto	154
Braga	102
Vila Nova de Gaia	86
Coimbra	85
More...	

Shares			Shares		
Name	Type	Comments	Name	Type	Comments
Web	Shares		ADMIN\$	Disk	Remote Admin
Public	Name	Type	C\$	Disk	Default Share
homes			IPC\$	Printer	
SCAN	Multimedia	Shares			
SERVER	Download	Name			
Multimedia	Web				
Recordings	Public	Multimedia			
home	homes	Download			
MBPT	TESTE	Web			
PLOUTOS	JOAO	Public			
TGS	DUDA	homes			
MIRUS	SEGMENTO_POPULAR	BackupR			
USB	SOFTWARE	home			
IPC\$	home	IPC\$			
	IPC\$				

Portugal

Shodan.io - Motor de busca - Internet Of Things

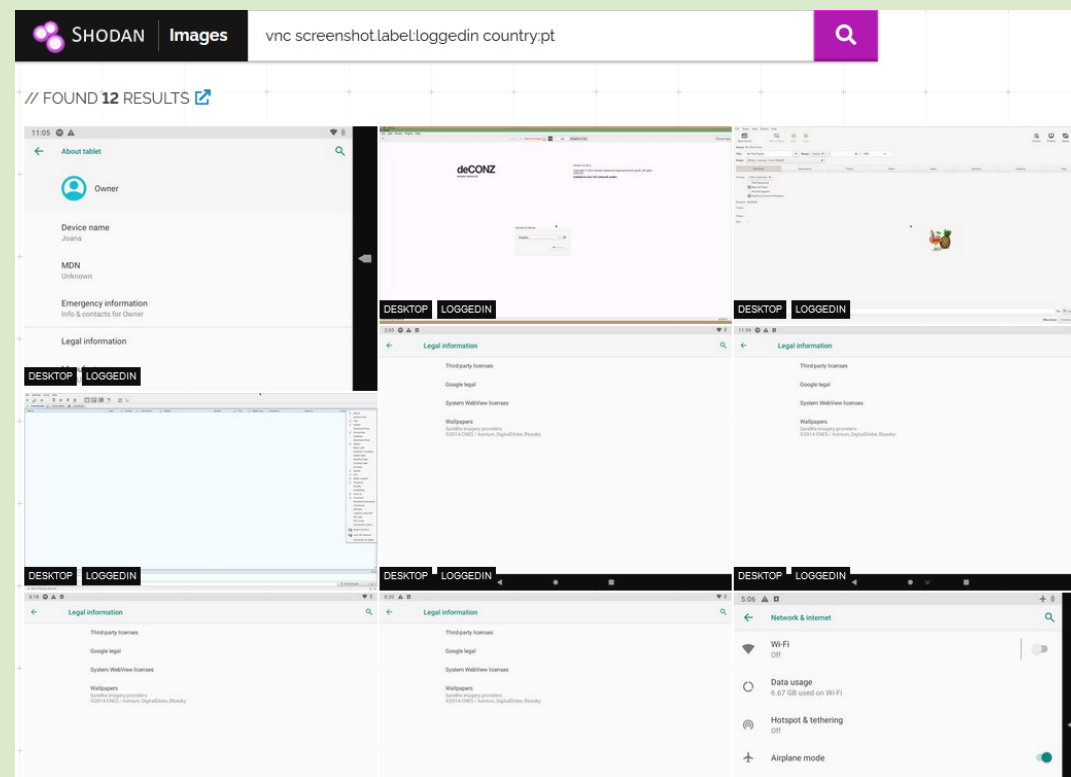
Acesso Remoto sem autenticação

TOTAL RESULTS

12

TOP CITIES

Porto	8
Lisbon	2
Cacém	1
Vila Nova de Gaia	1



Q&A