

# Deutschland Bier, Wurst und Schwachstellen

Open Identity Summit 2024



# \$whoami

- ▶ Pedro Vieira
- ▶ Cyber Security Engineer
- ▶ Certified Ethical Hacker
- ▶ Degree at University of Minho



# Disclaimer & Laws

# Disclaimer

## Boring but necessary

- ▶ Information in this presentation is intended for educational and awareness purposes only.
- ▶ **Live presentation.** Not a controlled environment and some contents may be inappropriate for some users.
- ▶ **I accept no responsibility** in any kind for the use, misuse, downloading, viewing in whatever way the links in this presentation.
- ▶ This presentation is **not related** to my work or employer.



# Disclaimer

## Avoid illegal activities

- ▶ Some links, websites, software or other items listed may or **may not be legal**, illegal, a felony, misdemeanor, or worse, in your country.
- ▶ Please make sure that you are **allowed** to browse the websites, download links and software **BEFORE USING!**
- ▶ Ignorance about laws or rules is **no excuse** for illegal activities or wrongdoing.
- ▶ Illegal activities may get you in **trouble or arrested**.
- ▶ Always check what is legal, and what laws apply.



# Laws

## Portuguese Law and Organizations

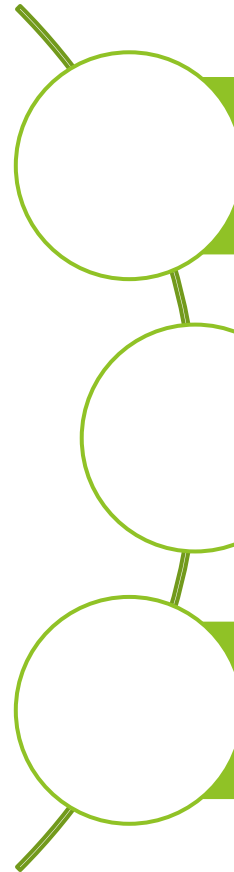
### ► Laws

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

### ► Organizations

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

# Agenda

- 
- Vulnerability
  - Common Attack Vectors
  - German Landscape

# Vulnerability

Definition and Statistics



# Vulnerability

## Vulnerability vs incident

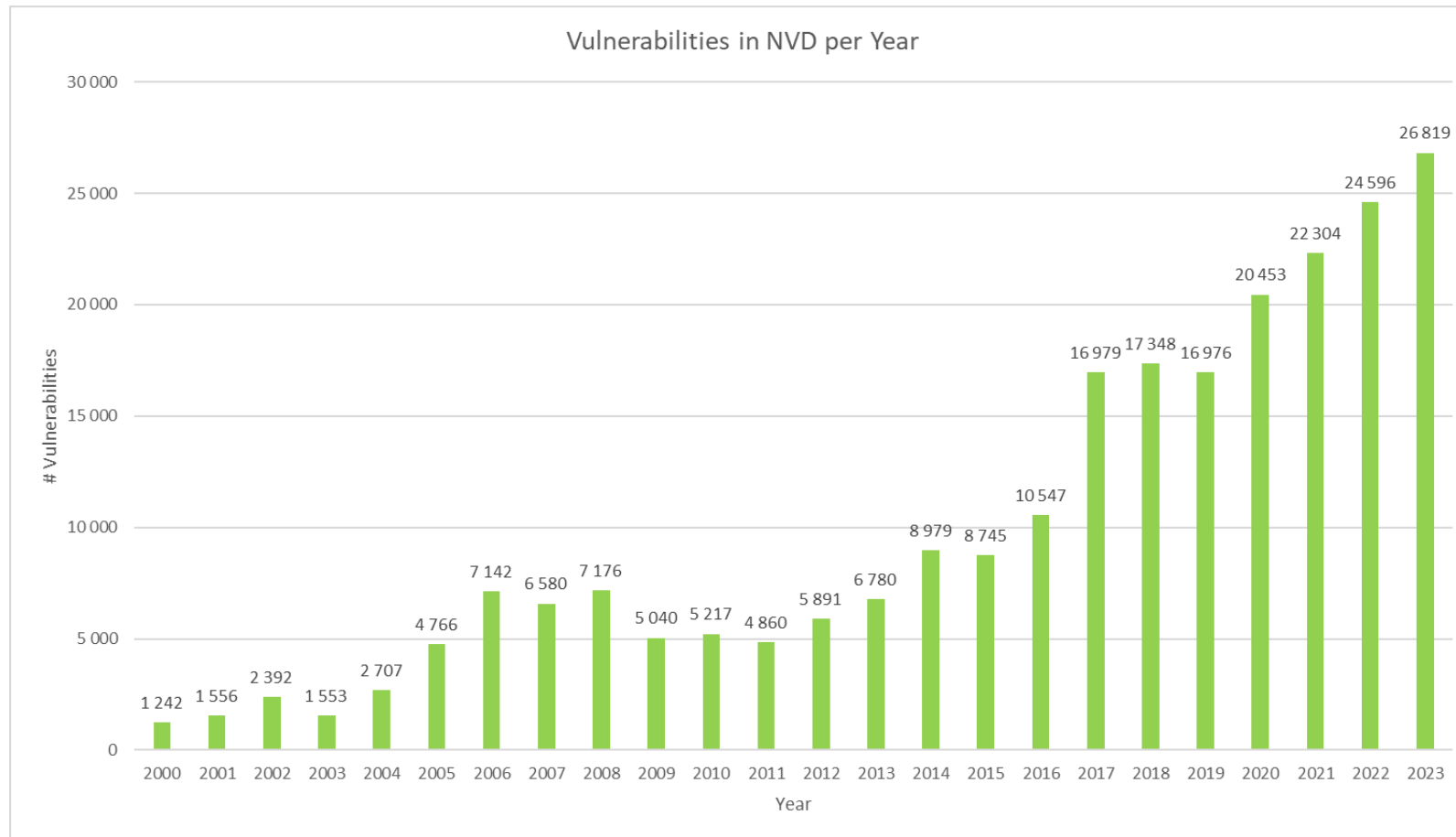
### Vulnerability

"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>

Vulnerability	Incident
Open door 	Unauthorized access 

# Vulnerability Statistics by Year

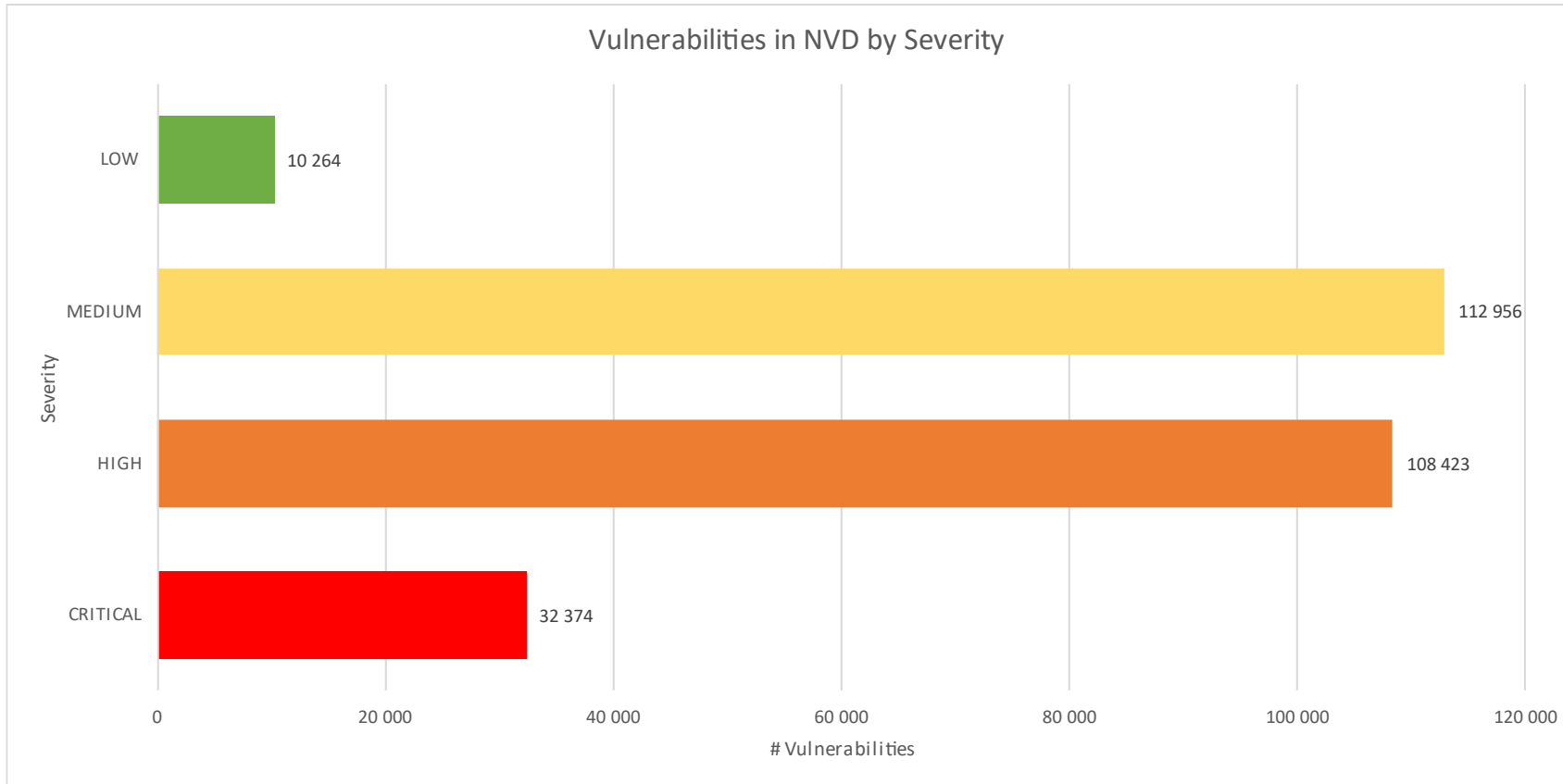


Total known vulnerabilities

**283.154**

Source NVD 14/03/2024

# Vulnerability Statistics by Severity



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

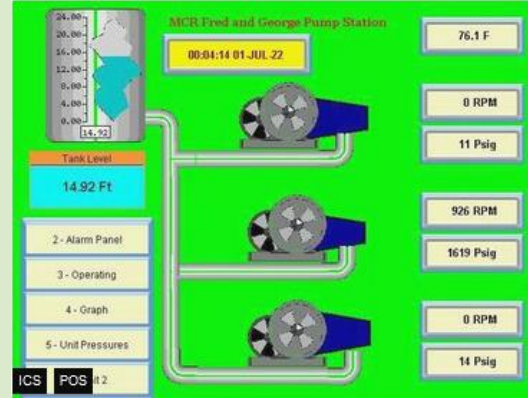
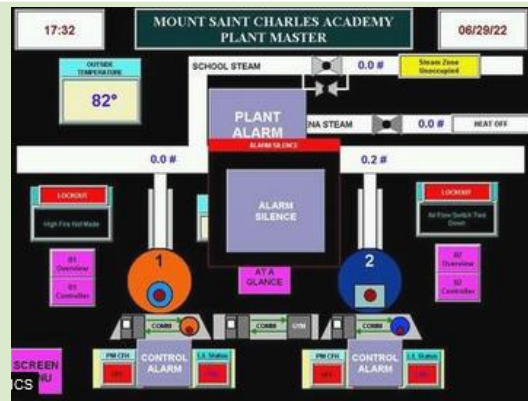
# Vulnerability

## Examples from Shodan.io

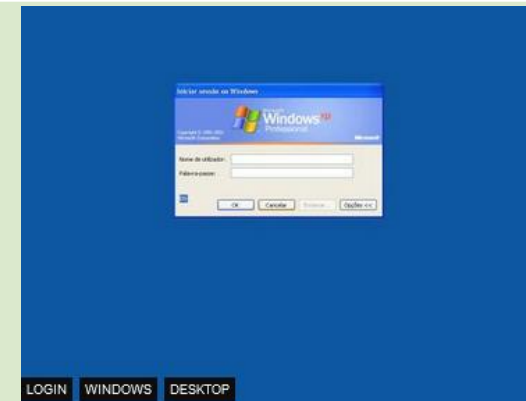
### Default/No Password



### Industrial Control Systems



### Vulnerable Systems



# Common Attack Vectors

Easy-Peasy

# Common Attack Vectors

## Credentials

[illegible]

# Common Attack Vectors

## Misconfiguration

### Shared Folder - Authentication disabled

<b>SMB Status:</b> <b>Authentication: disabled</b> SMB Version: 2 Capabilities: raw-mode		<b>SMB Status:</b> <b>Authentication: disabled</b> SMB Version: 2 Capabilities: raw-mode		<b>SMB Status:</b> <b>Authentication: disabled</b> 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

### Shared Folder - Remote Code Execution

#### 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	



# Common Attack Vectors

## Malware - Ransomware

Redeemer Ransomware	Ransomwatch
<div><p>Redeemer Ransomware - Your Data Is Encrypted</p><p>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</p><p>Made by Cerebrate Visit the official Redeemer Ransomware Tor website - redeemergd6jtzgiuf5jgpkk6i3xybkhsldzjoyjaxivy2lnhvmzcad.onion</p><p>[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.</p><p>[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).</p><p>[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.</p><p>OK</p></div>	<div><p>summary</p><p>may 4th, 2024</p><p>ransomwatch is currently crawling 382 sites belonging to 192 unique groups</p><p>⌚ there have been 31 posts within the last 24 hours</p><p>📅 there have been 64 posts within the month of may</p><p>🕒 there have been 1286 posts within the last 90 days</p><p>📅 there have been 1712 posts within the year of 2024</p><p>🔍 there are currently 100 online hosts &amp; 120 custom parsers.</p><p>📊 ransomwatch has been running for 2 years, 7 months and 28 days and indexed 11169 posts</p><p>all data (groups) and (posts) is available in JSON (updated hourly)</p><p>ransomwatch is fully open source. please consider sponsoring if you find it useful!</p></div>



# Common Attack Vectors

## Malware - Ransomware

### Ransomwatch

#### recent posts

last 200 posts

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

### NoMoreRansom

<🔒/> NO MORE RANSOM

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

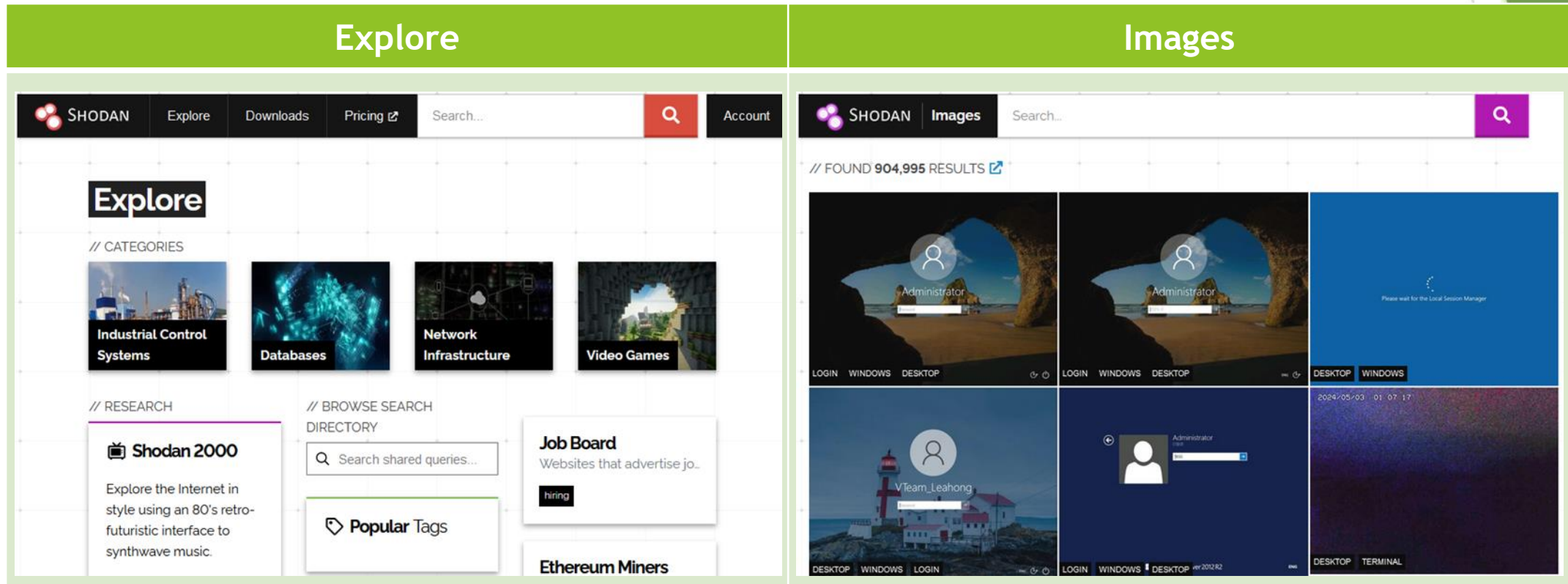
YES NO

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

# German landscape

# Germany

## Shodan.io - Search Engine for Internet Of Things

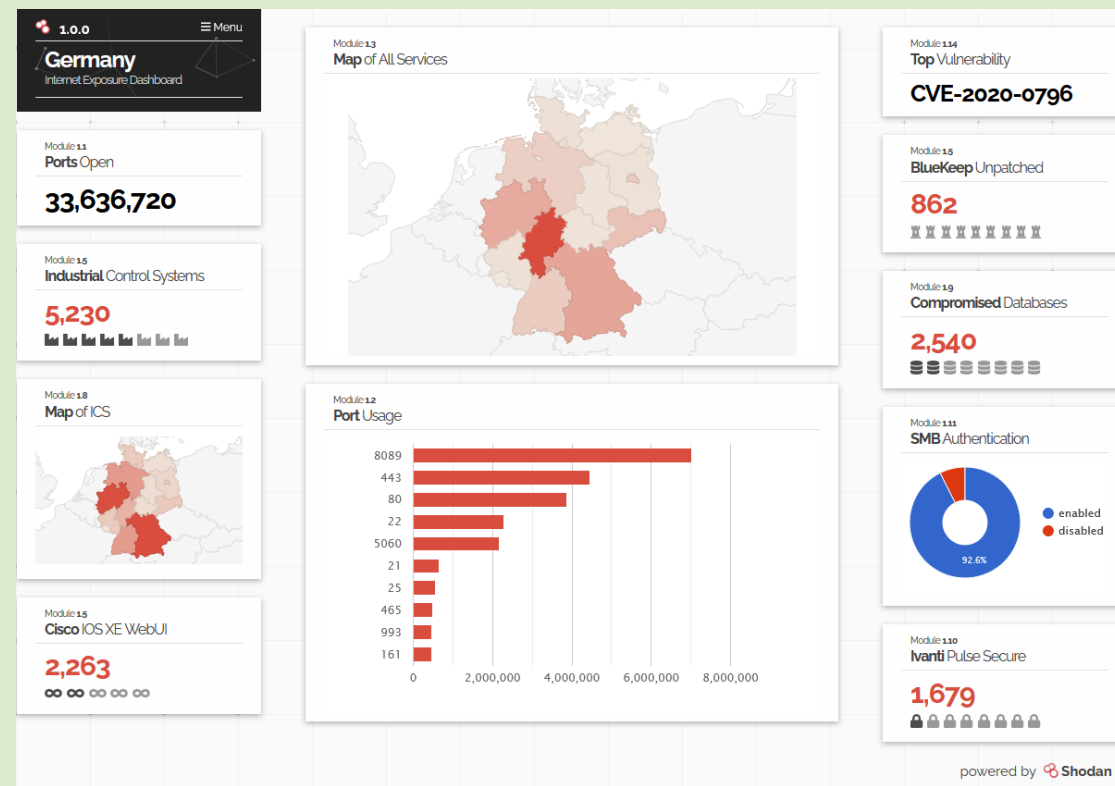


Shodan Queries ([link](#))

# Germany

## Shodan.io - Search Engine for Internet Of Things

### Internet Exposure Observatory



# Germany

## Shodan.io - Search Engine for Internet Of Things

### Top in Germany - 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

22,735

#### TOP CITIES

Berlin	7,836
Frankfurt am Main	5,048
Falkenstein	3,806
Düsseldorf	3,075
Nürnberg	1,340

[More...](#)

### EternalBlue - MS17-010 - CVE-2017-0144

#### Vulnerabilities

**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.

#### TOTAL RESULTS

215

#### TOP CITIES

Nürnberg	86
Frankfurt am Main	67
Falkenstein	26
Berlin	8
Düsseldorf	6

[More...](#)

# Germany

## Shodan.io - Search Engine for 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

4,844

#### TOP CITIES

Frankfurt am Main	973
Falkenstein	836
Berlin	732
Karlsruhe	413
Nürnberg	235

[More...](#)

### Logjam - CVE-2022-32548

#### Vulnerabilities

**CVE-2022-32548** 10.0 Unauthenticated Remote Code Execution in a Wide Range of DrayTek Vigor Routers

#### TOTAL RESULTS

4,225

#### TOP CITIES

Berlin	330
Hamburg	149
Frankfurt am Main	145
Düsseldorf	107
Munich	102

[More...](#)

# Germany

## Shodan.io - Search Engine for 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'.

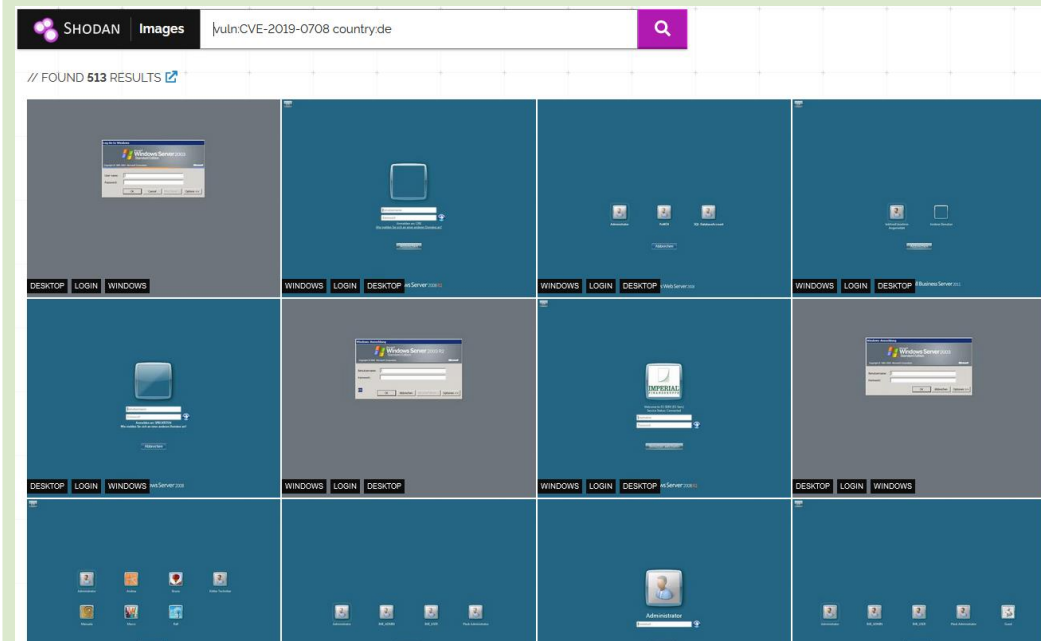
#### TOTAL RESULTS

905

#### TOP CITIES

Frankfurt am Main	234
Berlin	154
Düsseldorf	68
Falkenstein	63
Nürnberg	40

[More...](#)



# Germany

## Shodan.io - Search Engine for Internet Of Things

### Shared Folders

TOTAL RESULTS

5,044

TOP CITIES

Frankfurt am Main	1,616
Falkenstein	788
Nürnberg	646
Düsseldorf	516
Berlin	469

[More...](#)

Shares Name	Type	Comments
print\$	Disk	Printer Drivers
lobby	Disk	Lobby
freebuild	Disk	Freebuild
creative	Disk	Creative
redstone	Disk	Redstone-Server
hardcore	Disk	Hardcore-Server
iron	Disk	Iron-Server
backup	Disk	Goliath
IPC\$	IPC	IPC Ser

Shares Name	Type	Comments
seskayit	Disk	Ses Kayitlari
faks	Disk	Faks Kayitlari
moh	Disk	Bekletme Muzikleri
sesler	Disk	Sistem Ek Mesajlari
IPC\$	IPC	IPC Service (IPS File Server)

Shares Name	Type	Comments
backup	Disk	Intra2net Business Server backup
restore	Disk	Intra2net Business Server backup restore
IPC\$	IPC	IPC Service (Intra2net - i2n)

Shares Name	Type	Comments
ADMIN\$		
C\$		
IPC\$		

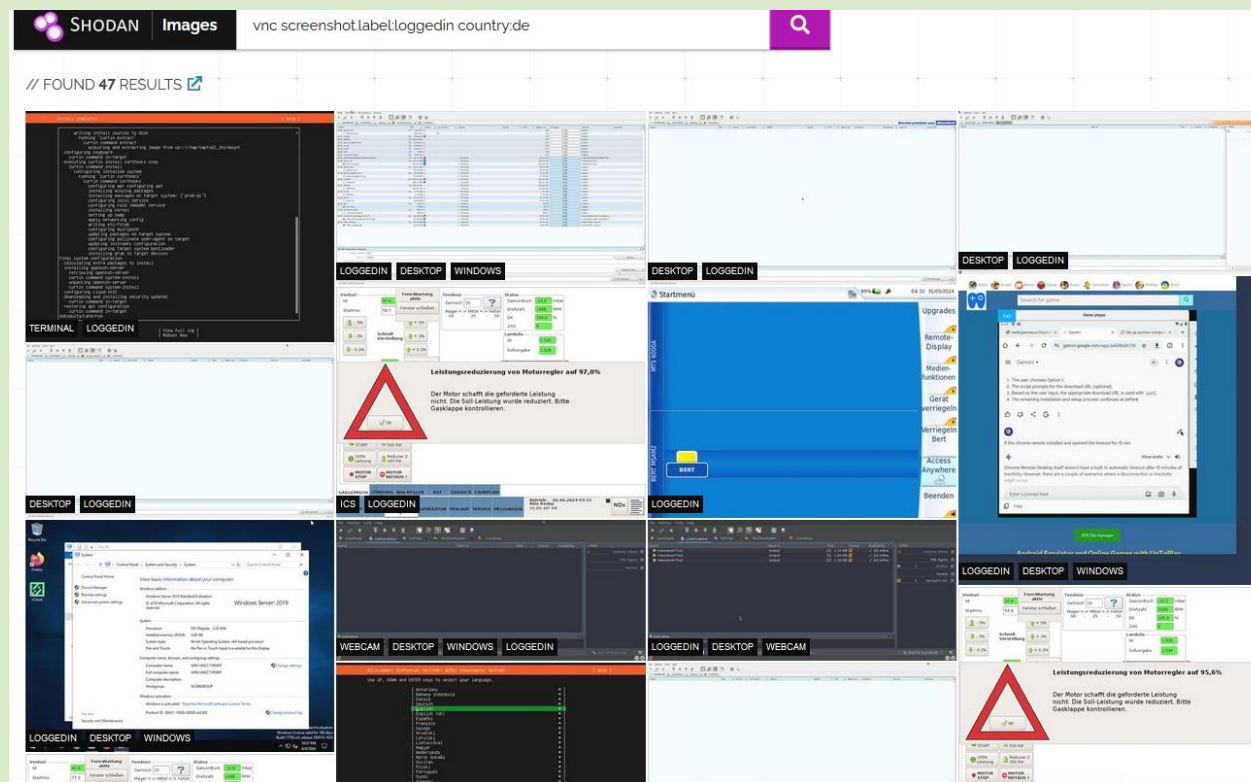
Shares Name	Type	Comments
logs	Disk	The recieved log files from customers.
IPC\$	IPC	IPC Service (Ubuntu-1804-bionic-64-minimal server (Samba, Ubuntu))



# Germany

## Shodan.io - Search Engine for Internet Of Things

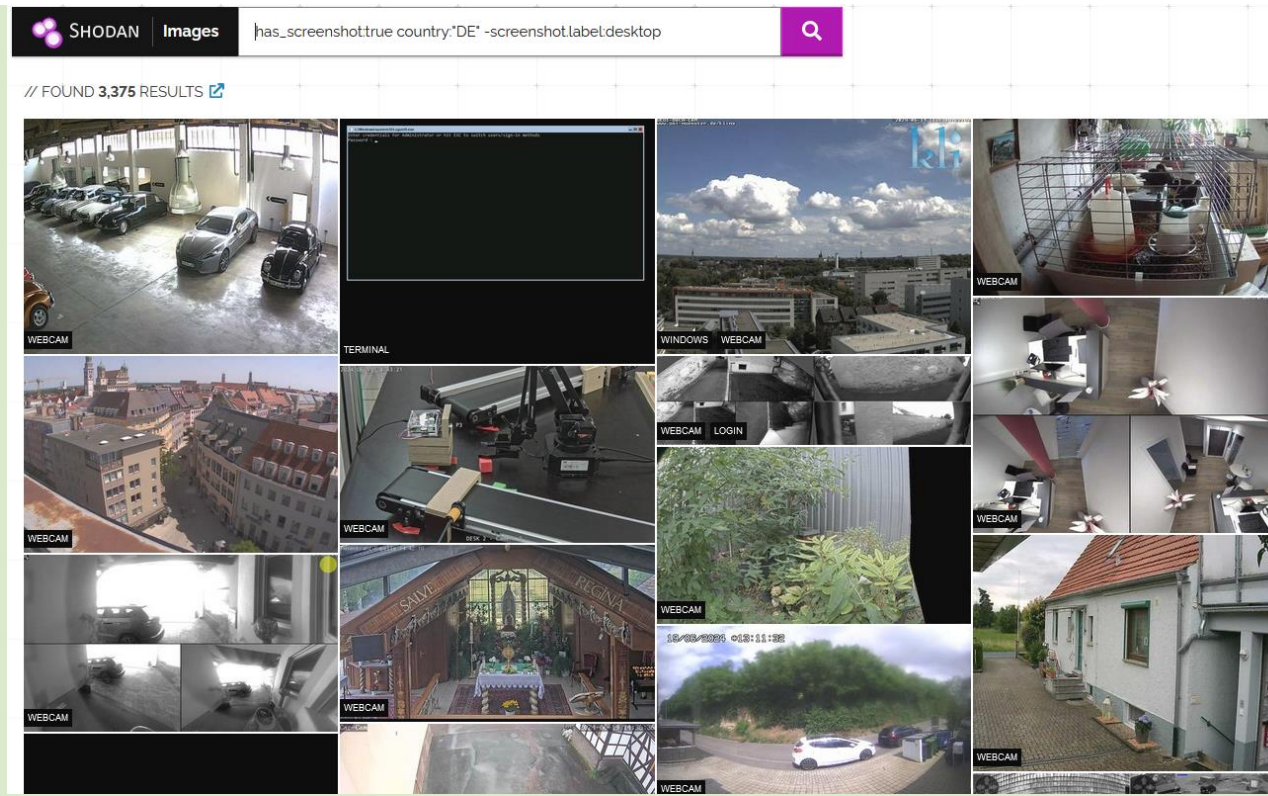
### Logged In Remote Access



# Germany

## Shodan.io - Search Engine for Internet Of Things

### Webcam



# THANK YOU

## Q&A

