



# SEMINÁRIO CIBERSEGURANÇA

- Miguel Santareno
- Offensive Security Manager – PwC Portugal

# ÍNDICE:

- Ataques de ransomware – antes
- Ataques de ransomware – após
- Ataques de defacement
- Partilha de informação entre organismos públicos

# ATAQUES DE RANSOMWARE - ANTES

Ransomware é um tipo de malware que encripta os dados e o grupo responsável pelo ataque pede um resgate para os dados serem decifrados e por sua vez se o resgate não for pago os dados são expostos na dark net.

# ATAQUES DE RANSOMWARE - ANTES

The screenshot shows a ransomware website interface. At the top left is the logo for 'LOCKBIT 3.0'. To its right is a red banner with the text 'LEAKED DATA'. Further right is a navigation menu with links for 'TWITTER', 'CONTACT US', 'AFFILIATE RULES', 'HOW TO BUY BITCOIN', 'PRESS ABOUT US', and 'MIRRORS'. The main content area features a large red timer displaying '3D18H13M26S' in white text, with the words 'UNTIL FILES' above and 'PUBLICATION' below. At the bottom of the page, a red text line indicates the deadline: 'Deadline: 01 Aug, 2022 03:22:30 UTC'.

**LOCKBIT 3.0**

**LEAKED DATA**

TWITTER  
CONTACT US  
AFFILIATE RULES

HOW TO BUY BITCOIN  
PRESS ABOUT US  
MIRRORS

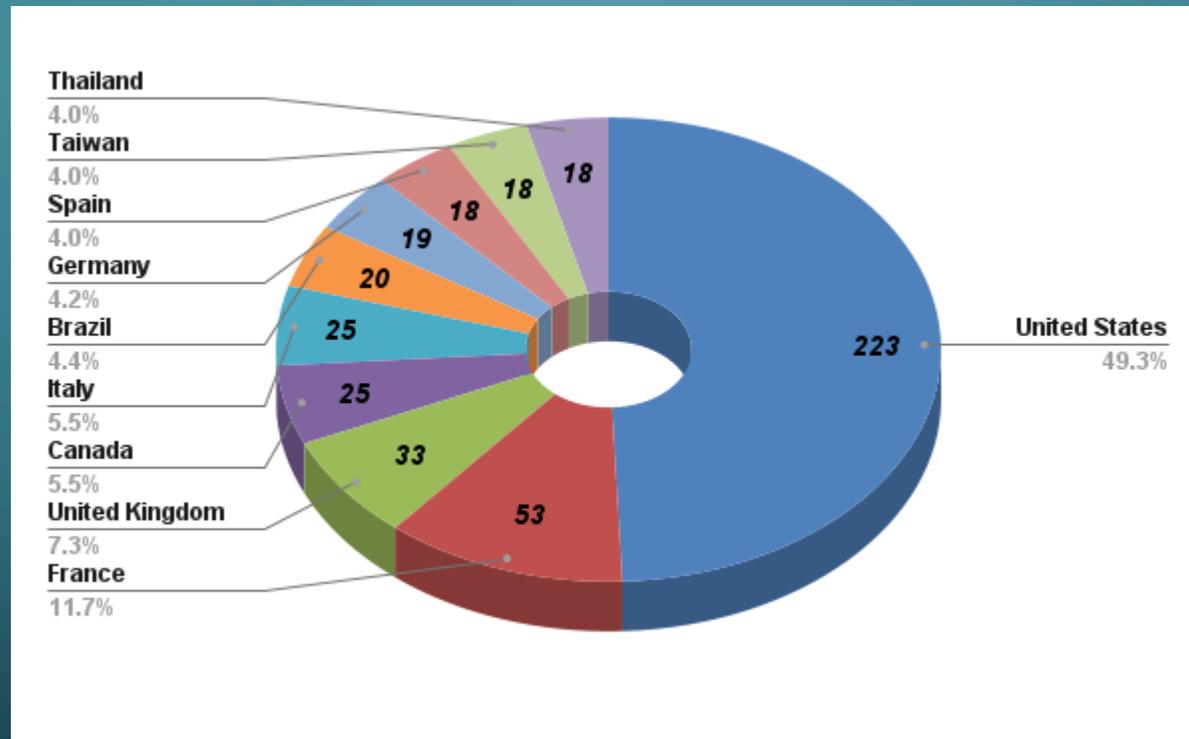
UNTIL FILES

**3D18H13M26S**

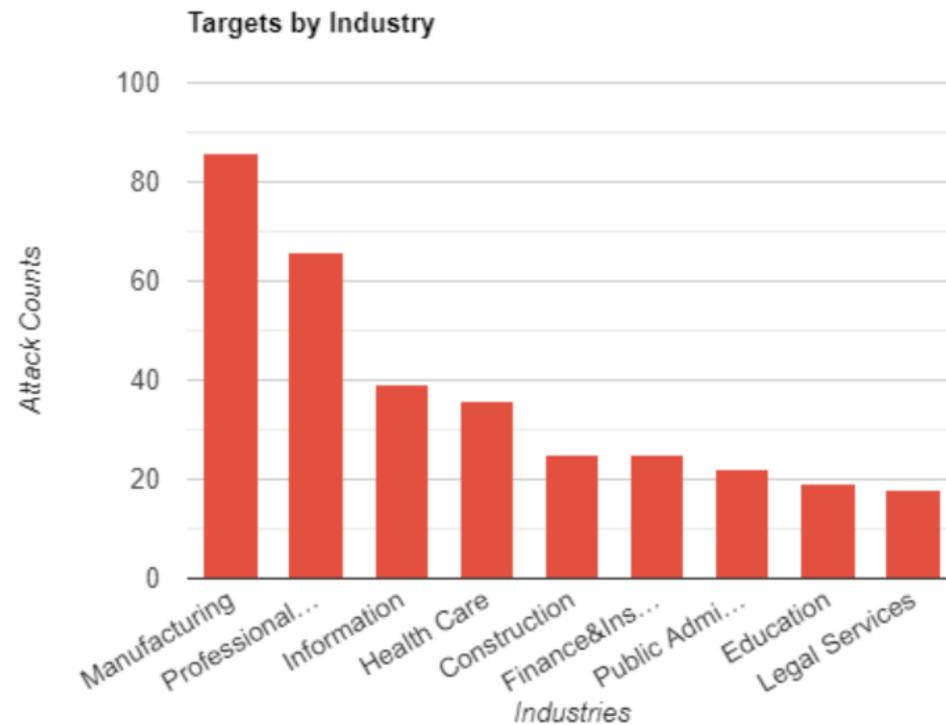
PUBLICATION

Deadline: 01 Aug, 2022 03:22:30 UTC

# ATAQUES DE RANSOMWARE - ANTES



# ATAQUES DE RANSOMWARE - ANTES



Top targeted industries by LockBit 3.0

# ATAQUES DE RANSOMWARE - ANTES

## MITRE ATT&CK TTPs

Tactics	Technique	ID
Initial Access	Valid Accounts	T1078
Exploit External Remote Services	T1133	
Drive-by Compromise	T1189	
Exploit Public-Facing Application	T1190	
Phishing	T1566	
Execution	Execution	TA0002
Software Deployment Tools	T1072	

# ATAQUES DE RANSOMWARE - ANTES

Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)
Phishing (0/3)	Exploitation for Client Execution	Browser Extensions
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary
Supply Chain Compromise (0/3)	Native API	Create Account (0/3)
Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)
	Serverless Execution	Event Triggered Execution (0/16)
	Shared Modules	External Remote Services
Valid Accounts (0/4)	Software Deployment Tools	Hijack Execution Flow (0/12)
	System Services (0/2)	Implant Internal Image
	User Execution (0/3)	Modify Authentication Process (0/8)
	Windows Management Instrumentation	Office Application Startup (0/6)
		Pre-OS Boot (0/5)
		Scheduled Task/Job (0/5)
		Server Software Component (0/5)
		Traffic Signaling (0/2)
		Valid Accounts (0/4)

# ATAQUES DE RANSOMWARE - ANTES

Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques
Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)
Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)
External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)
Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)
Phishing (0/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)
Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)
Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host
Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)
	Serverless Execution	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation
Valid Accounts (0/4)	Shared Modules	External Remote Services	Hijack Execution Flow (0/12)
	Software Deployment Tools	Hijack Execution Flow (0/12)	Process Injection (0/12)
	System Services (0/2)	Implant Internal Image	Scheduled Task/Job (0/5)
	User Execution (0/3)	Modify Authentication Process (0/8)	Valid Accounts (0/4)
	Windows Management Instrumentation	Office Application Startup (0/6)	
		Pre-OS Boot (0/5)	
		Scheduled Task/Job (0/5)	
		Server Software Component (0/5)	
		Traffic Signaling (0/2)	
		Valid Accounts (0/4)	

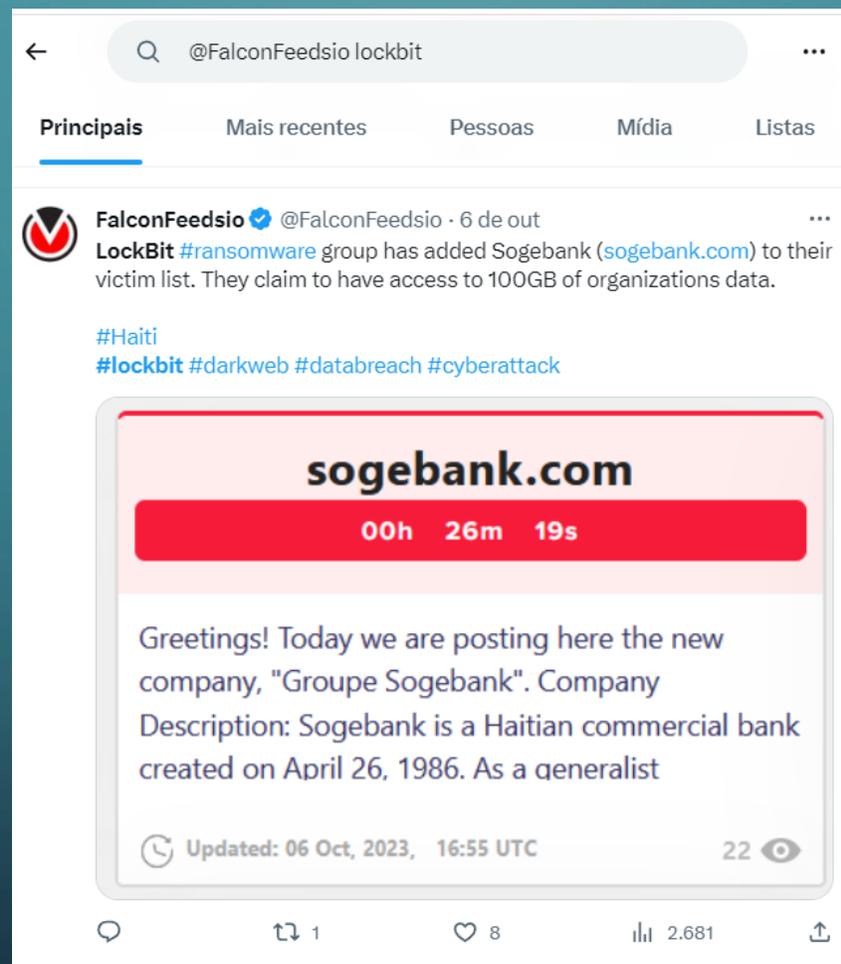
# ATAQUES DE RANSOMWARE - ANTES

- Realizados de forma recorrente e validados antecipadamente se não estão comprometidos.
- A Regra 3-2-1-1-0 recomenda que haja pelo menos três cópias dos dados importantes, em pelo menos dois tipos de mídia, com pelo menos uma cópia off-site.

# ATAQUES DE RANSOMWARE - APÓS

- Manter a calma.
- Desligar a infraestrutura da internet e isolar a mesma.
- Contatar uma empresa que contenha uma equipa de resposta a incidentes e sistemas.
- Contatar a PJ, CNCS e CNPD.
- Contatar parceiros e stakeholders.

# ATAQUES DE RANSOMWARE - APÓS



# ATAQUES DE RANSOMWARE - APÓS

The screenshot shows a web browser window with the address bar displaying a Tor-style URL: `lockbitapt2d73krlbewgv27tquljgxr33xbwwsp6rkyieto7u4ncead.onion`. The page content is organized into three columns, each representing a different target website. Each column has a header with the website name, a 'PUBLISHED' status indicator, a descriptive paragraph, and a timestamp with a view count.

Target Website	Status	Description	Updated	Views
<b>sogebank.com</b>	PUBLISHED	Greetings! Today we are posting here the new company, "Groupe Sogebank". Company Description: Sogebank is a Haitian commercial bank created on April 26, 1986. As a	Updated: 09 Oct, 2023, 08:18 UTC	402
<b>eclipse-print.com</b>	PUBLISHED	ECLIPSE GROUP is a large-scale manufacturer of a large-scale graphics with high-end service for each client.	Updated: 09 Oct, 2023, 08:17 UTC	30708
<b>ocrex.com</b>	PUBLISHED	OCREX was formed in 2009 and specialises in the development of OCR software solutions. OCREX has developed AutoRec which automates the process of performing bank	Updated: 09 Oct, 2023, 08:17 UTC	33795

# ATAQUES DE DEFACEMENT

- Um defacement ocorre quando um ator malicioso consegue alterar o conteúdo de um website normalmente com o intuito de se vangloriar-se do mesmo e não causar dano monetário.

# ATAQUES DE DEFACEMENT



# ATAQUES DE DEFACEMENT



Home News Events Archive Archive ★ Onhold Notify Stats Register Login

NOTIFIER  DOMAIN

Special defacements only  Fulltext/Wildcard  Onhold (Unpublished) only

Date :

Total notifications: **22** of which **22** single ip and **0** mass defacements

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
L - IP address location  
★ - Special defacement (special defacements are important websites)

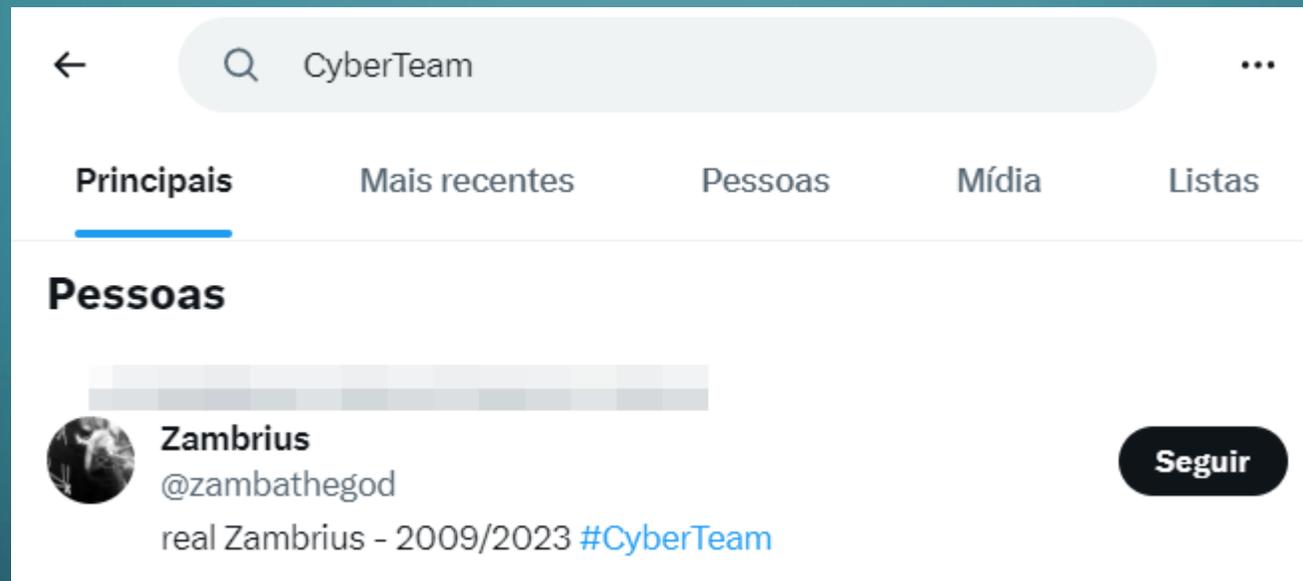
**We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.**

Time	Notifier	H	M	R	L	★ Domain	OS	View
2022/10/01	-1	H				★ mysns.sns.gov.pt	Linux	<a href="#">mirror</a>
2022/06/26	-1	H				★ ds3.sns.gov.pt	Linux	<a href="#">mirror</a>
2022/03/27	Mr.Kro0oz.305			R		★ portaldaenergia.azores.gov.pt/...	FreeBSD	<a href="#">mirror</a>
2021/03/27	Mr.Kro0oz.305					★ portaldaenergia.azores.gov.pt/...	Linux	<a href="#">mirror</a>
2020/03/18	LAMERTeam					★ bibliografia.bnportugal.gov.pt...	Win 2008	<a href="#">mirror</a>
2020/01/27	CyberTeam			R		★ parquesnaturais.azores.gov.pt/...	Win 2008	<a href="#">mirror</a>
2020/01/20	Panataran	H				★ ebiap.edu.azores.gov.pt	Linux	<a href="#">mirror</a>
2019/11/19	CyberTeam					★ www.sg.mai.gov.pt/Paginas/defa...	F5 Big-IP	<a href="#">mirror</a>
2019/04/28	Anon Ghost Portugal			R		★ www.acessibilidade.gov.pt/acce...	Linux	<a href="#">mirror</a>
2018/02/12	Anon Ghost Portugal			R		★ parquesnaturais.azores.gov.pt/...	Win 2008	<a href="#">mirror</a>
2017/08/18	spl0it3r			R		★ www.portugal.gov.pt/pt.aspx	Linux	<a href="#">mirror</a>
2017/01/18	fsecurity	H		R		★ clai.acidi.gov.pt	Linux	<a href="#">mirror</a>
2017/01/18	Tsunami Faction	H				★ adctb.dglab.gov.pt	Linux	<a href="#">mirror</a>
2017/01/09	SudoDk			R		★ www.ccdr-a.gov.pt/alentejoape/	Linux	<a href="#">mirror</a>
2016/06/12	CyberTeam	H				★ www.madeira.gov.pt	Win 2012	<a href="#">mirror</a>
2016/06/12	CyberTeam	H		R		★ www.azores.gov.pt	Win 2003	<a href="#">mirror</a>
2016/06/01	LGH					★ www.acessibilidade.gov.pt/acce...	Linux	<a href="#">mirror</a>
2015/12/14	ProtoWave Reloaded	H				★ www.eslr.edu.azores.gov.pt	Win 2003	<a href="#">mirror</a>
2015/10/17	LophT Crews			R		★ parquesnaturais.azores.gov.pt/...	Win 2008	<a href="#">mirror</a>
2015/10/08	LuXas			R		★ www.portugal.gov.pt/pt.aspx	Linux	<a href="#">mirror</a>
2015/09/14	ProtoWave Reloaded	H				★ webb.ccdr-a.gov.pt	Linux	<a href="#">mirror</a>
2015/07/21	MR.XAMD					★ portal.pcp.pt/wordpress/	Linux	<a href="#">mirror</a>

1

**DISCLAIMER:** all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. [Read more](#)

# ATAQUES DE DEFACEMENT



# ATAQUES DE DEFACEMENT

expresso.pt/sociedade/2022-01-12-A-historia-e-a-longa-lista-de-crimes-de-Zambrius-o-jovem-hacker-da-Ericeira-que-vivia-com-os-pais-e-a-avo--e-foi-condenado-a-seis-anos-de-prisao--b04fadb6

EXCLUSIVOS SEMANÁRIO **Expresso50** INSERIR CÓDIGO

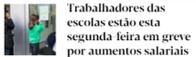
Tomás Pedroso, mais conhecido por Zambrius entre a comunidade de hackers internacional, fundou a equipa de piratas informáticos denominada Cyberteam, que existe desde 2011 mas que se popularizou em 2019 e 2020, com ataques em Portugal e no Brasil.

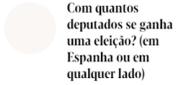
Tornaram-se famosos com os ataques DDOS, dirigidos a servidores, os Defacement of Websites, danificando páginas de Internet, e os SQL-Injection, explorando vulnerabilidades de sites. Foi agora condenado a seis anos de prisão por ter cometido 28 crimes de acesso ilegítimo agravado, desvio de dados e dano informático no espaço de dez meses.

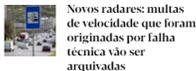
O jovem de 21 anos, que vive na Ericeira em casa dos pais e da avó materna, ficou em prisão domiciliária entre maio e novembro de 2020, e foi nessa condição que acabou detido pela PJ em novembro desse mesmo ano. Aconteceu no âmbito de uma operação conjunta com a Polícia federal brasileira por suspeitas de invasão no Tribunal Superior Eleitoral (TSE) do Brasil, durante a primeira volta das eleições autárquicas.

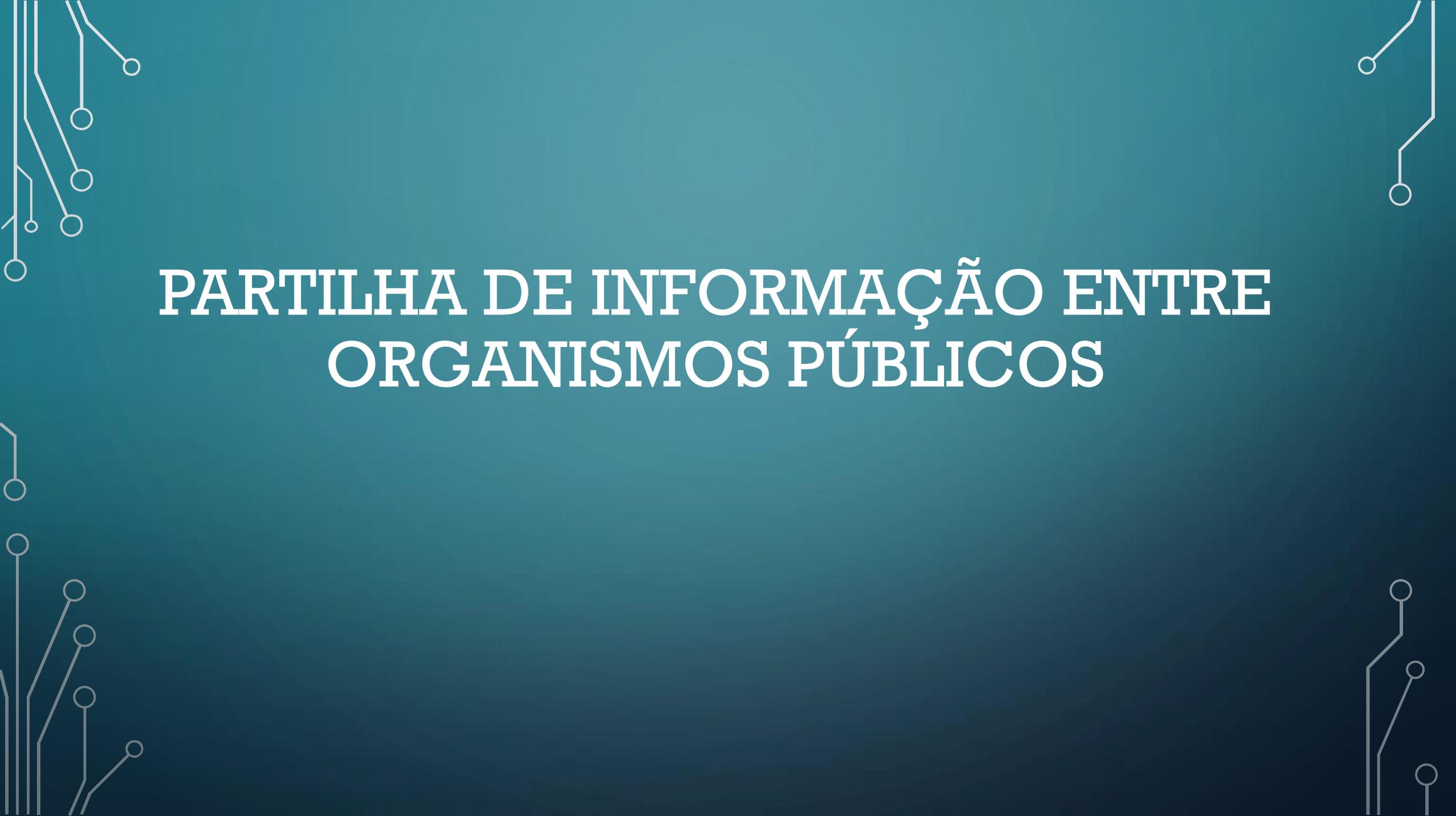
Zambrius já fora detido em 2017, com 16 anos, e internado até aos 18 anos num Centro Educativo: o jovem envolveu-se numa operação conduzida por vários hackers que tinham invadido as estruturas do Estado, como a PJ e a Procuradoria-Geral da República.

No acórdão do tribunal que agora o condenou por crimes informáticos, e a que o Expresso teve acesso, é referido que o seu ambiente familiar se caracteriza pela "harmonia e a existência de laços de solidariedade e entreaduda". A Tomás Pedroso foi-lhe diagnosticado déficit de atenção e hiperatividade e dificuldades em se socializar.

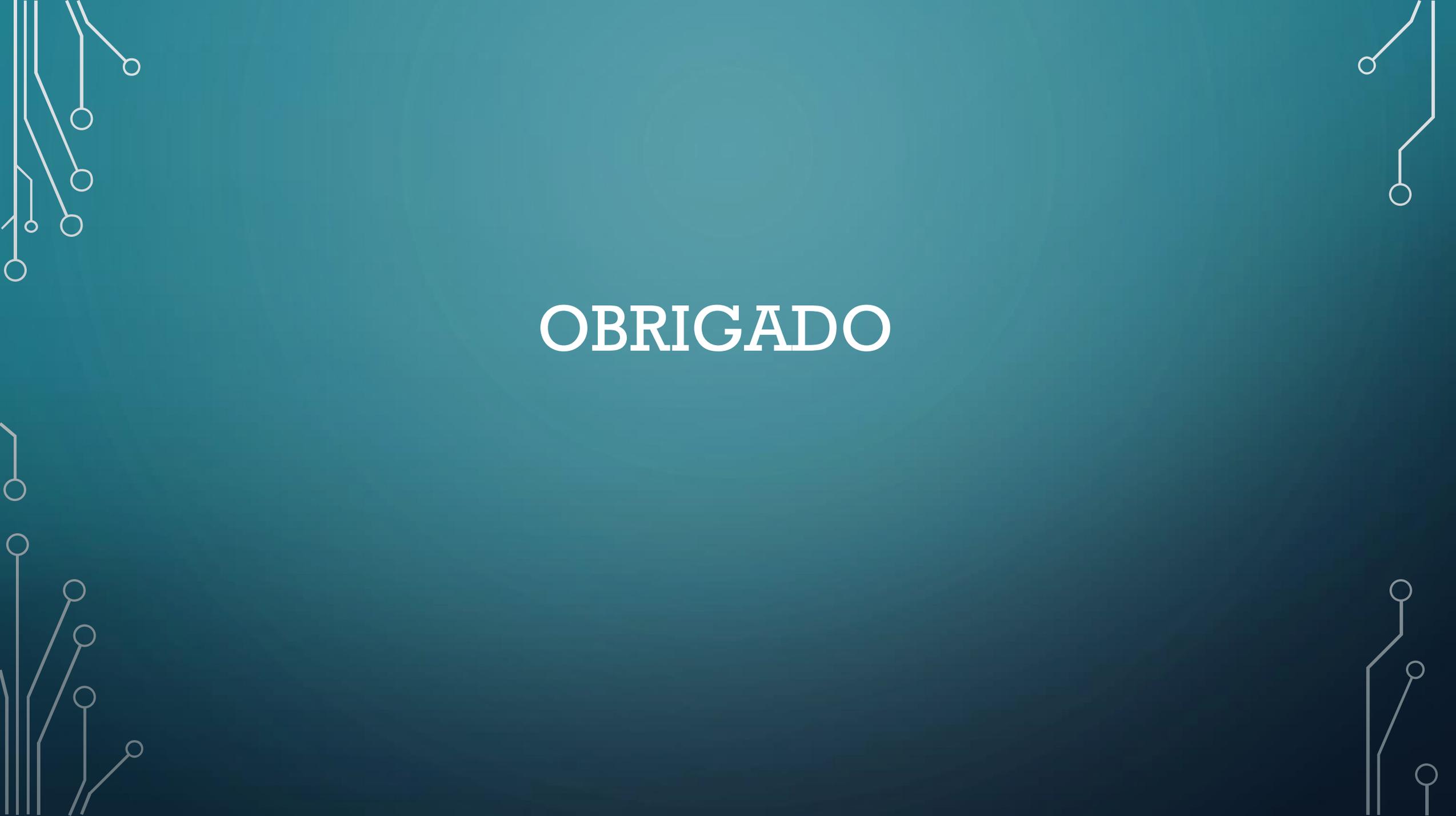








# PARTILHA DE INFORMAÇÃO ENTRE ORGANISMOS PÚBLICOS



OBRIGADO