SEMINÁRIO CIBERSEGURANÇA

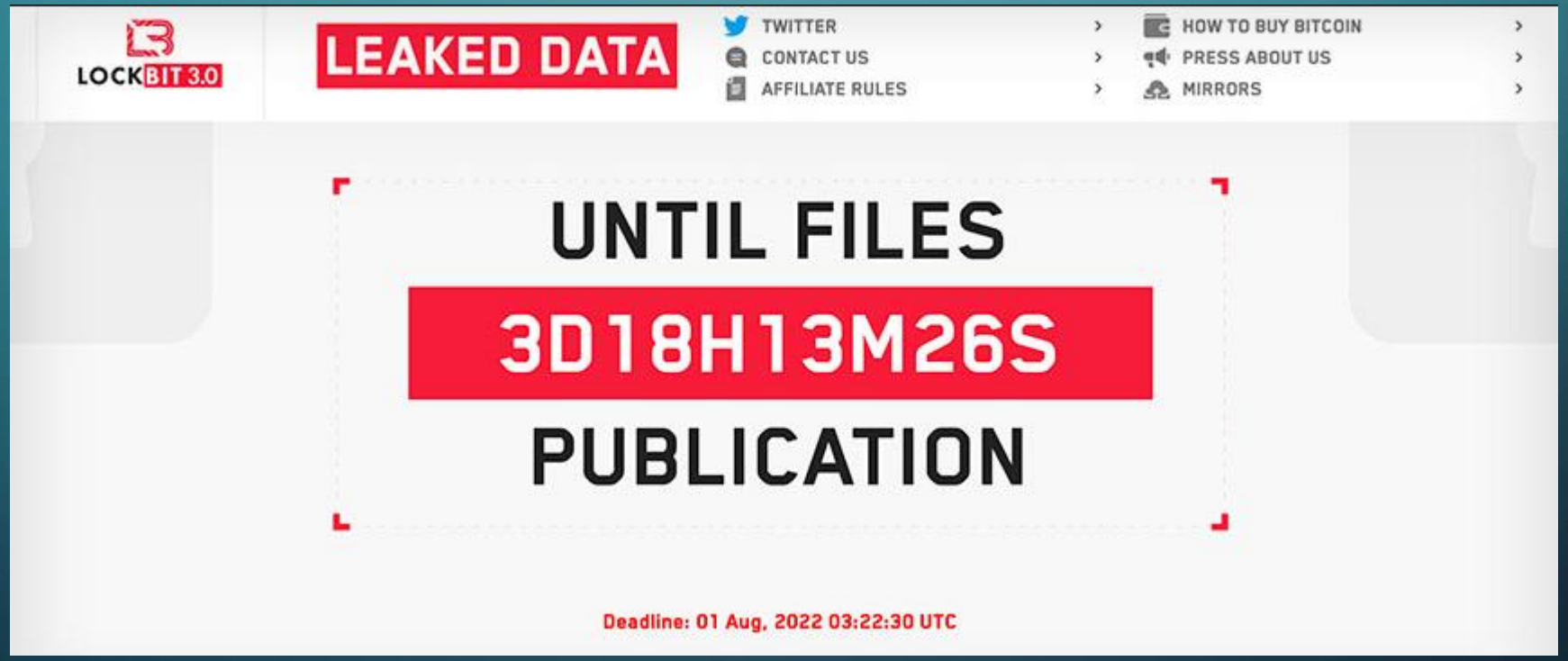
- Miguel Santareno
- Offensive Security Manager – PwC Portugal

ÍNDICE:

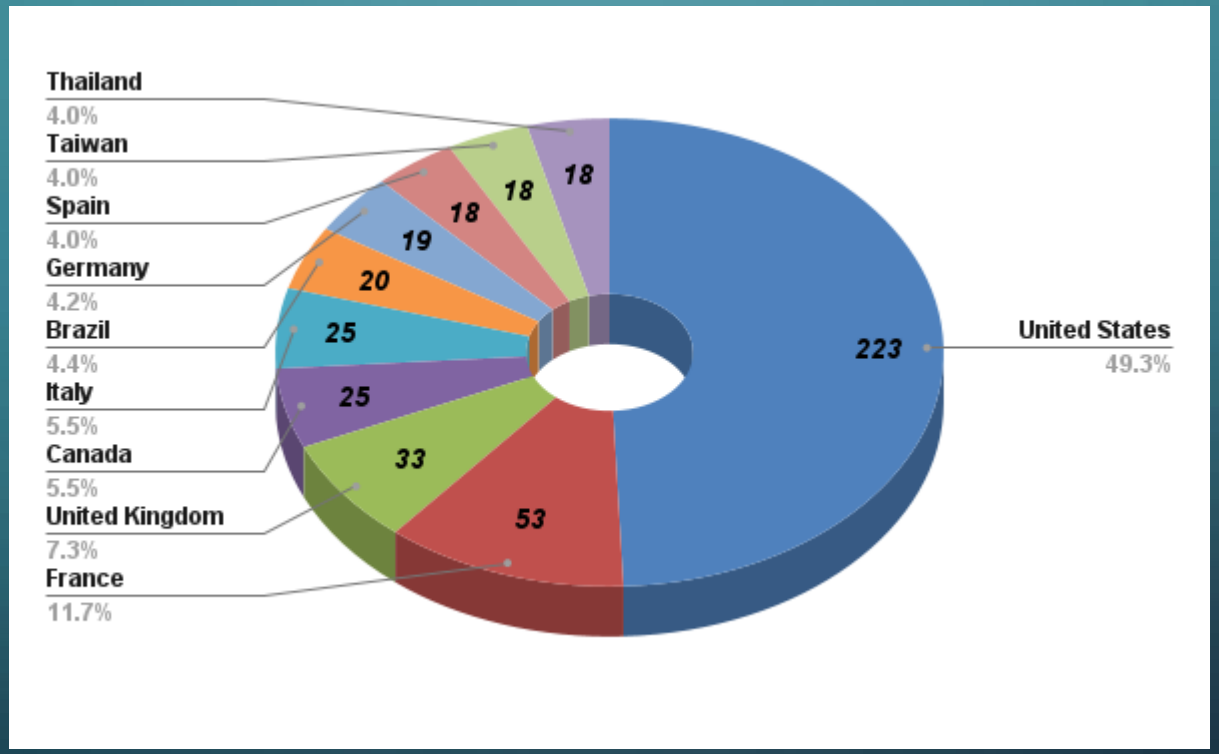
ATAQUES DE RANSOMWARE - ANTES

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.

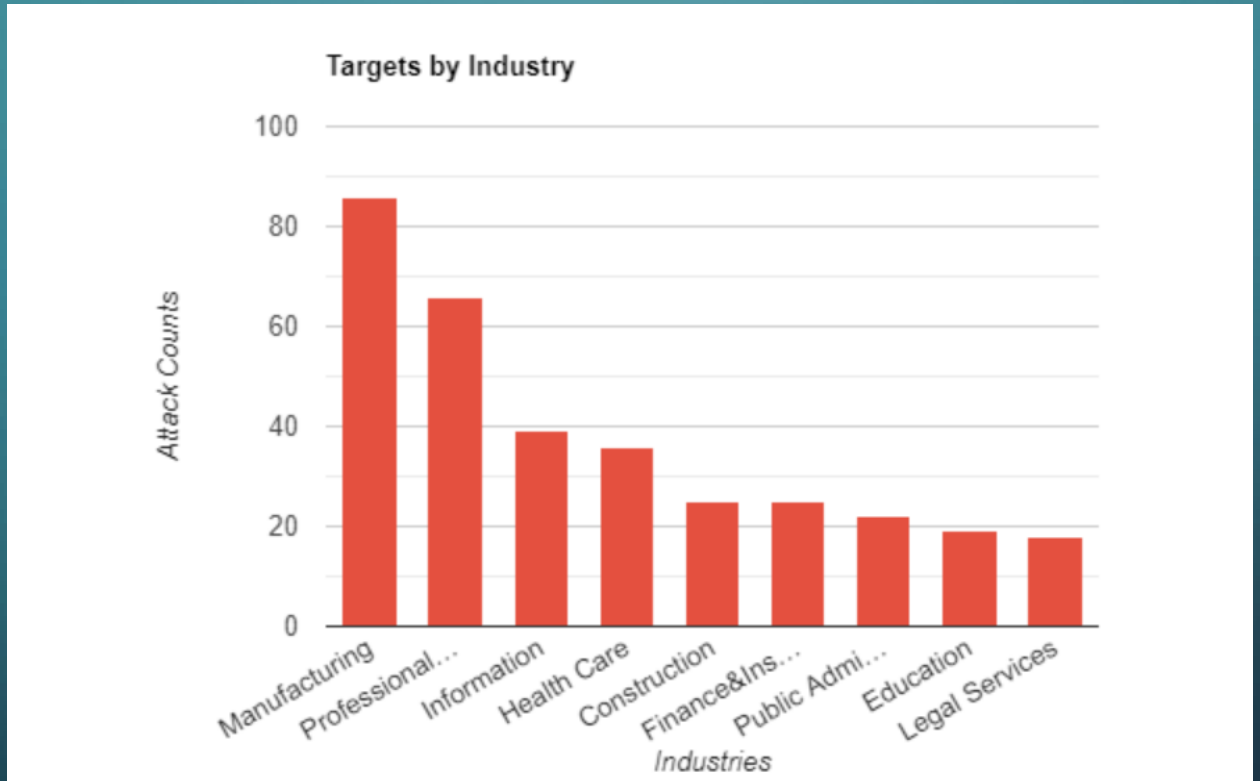
ATAQUES DE RANSOMWARE - ANTES



ATAQUES DE RANSOMWARE - ANTES



ATAQUES DE RANSOMWARE - ANTES



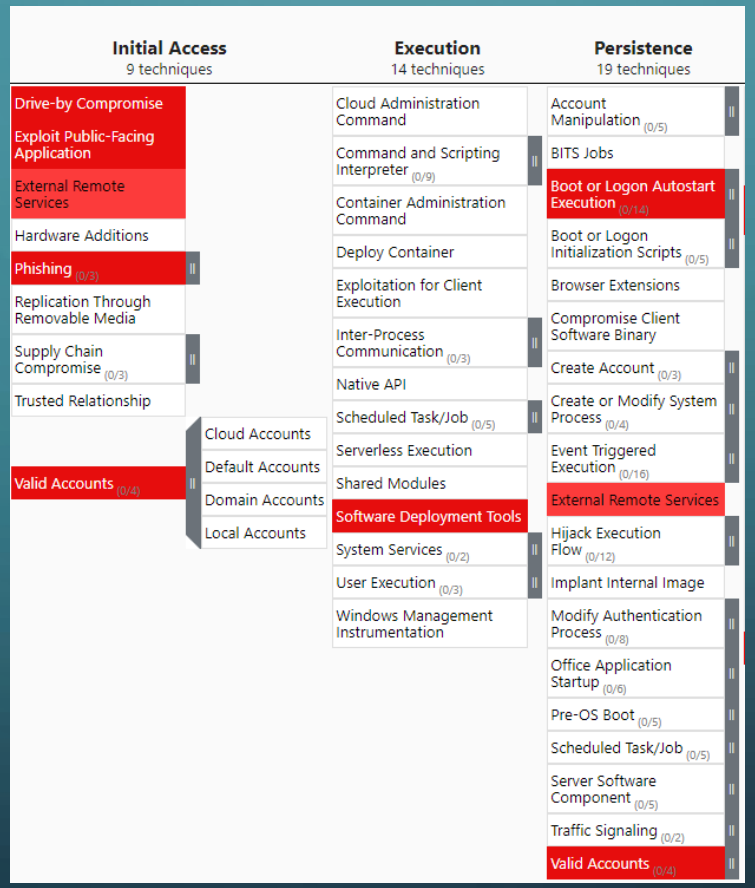
Top targeted industries by LockBit 3.0

ATAQUES DE RANSOMWARE - ANTES

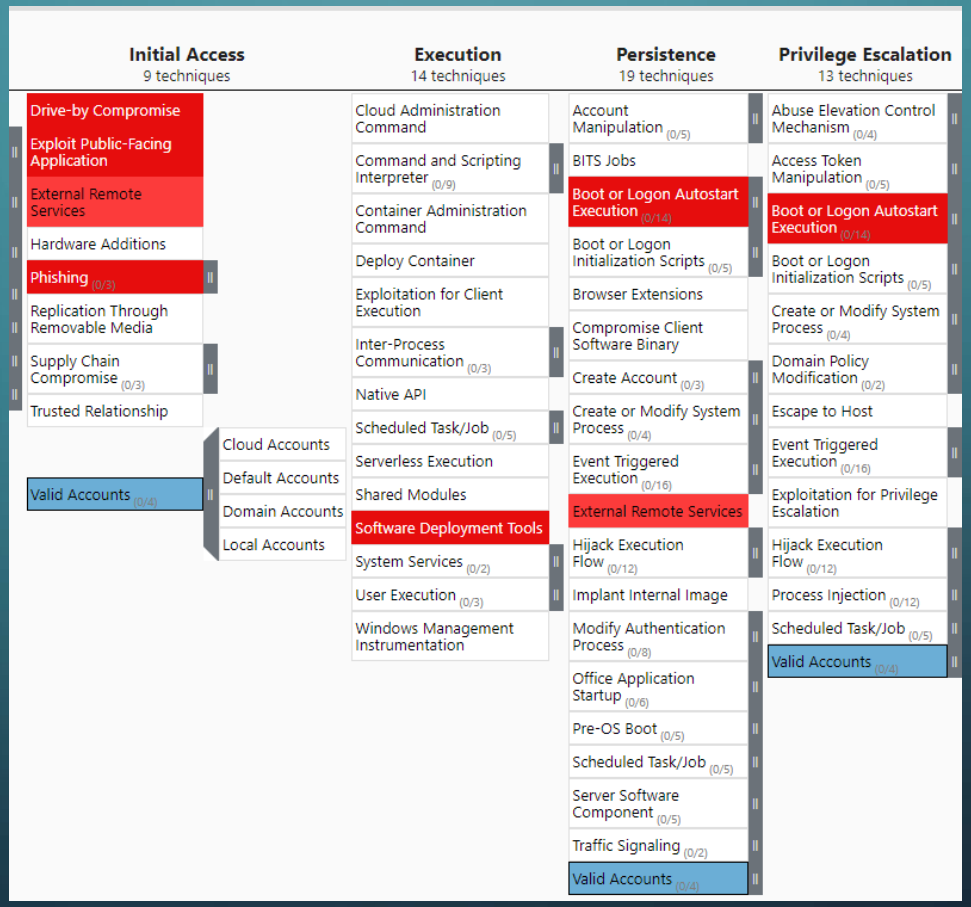
MITRE ATT&CK TTPs

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



ATAQUES DE RANSOMWARE - ANTES



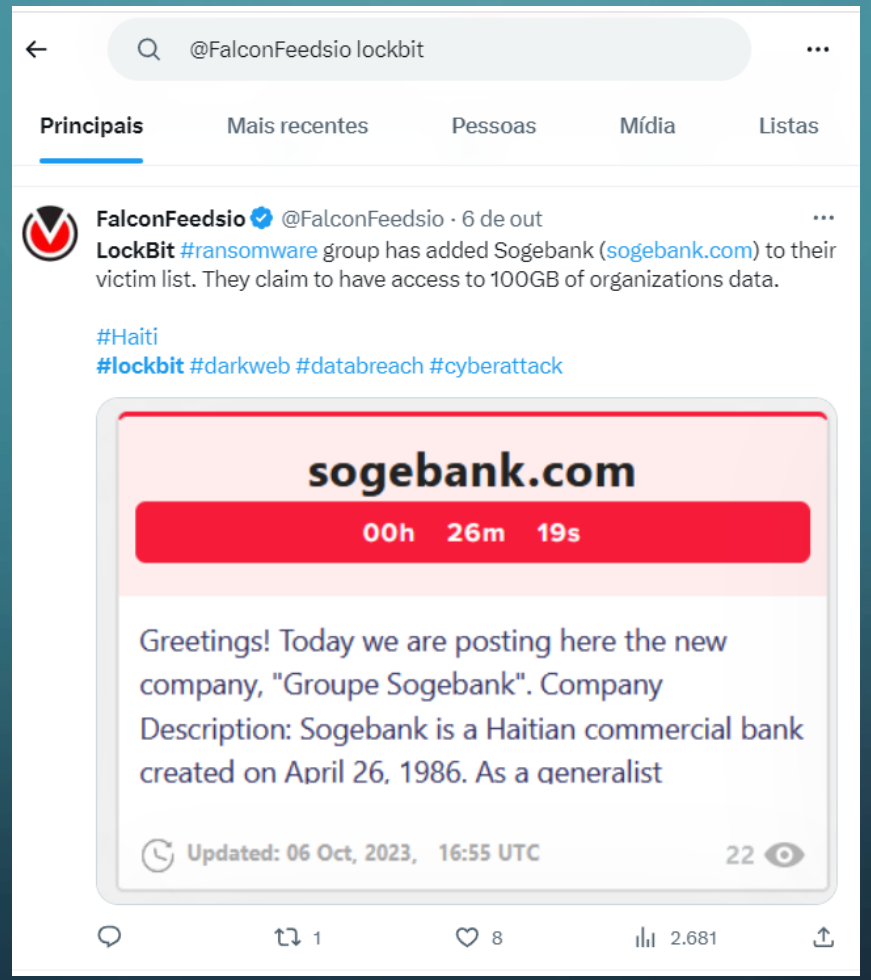
ATAQUES DE RANSOMWARE - ANTES

- 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.

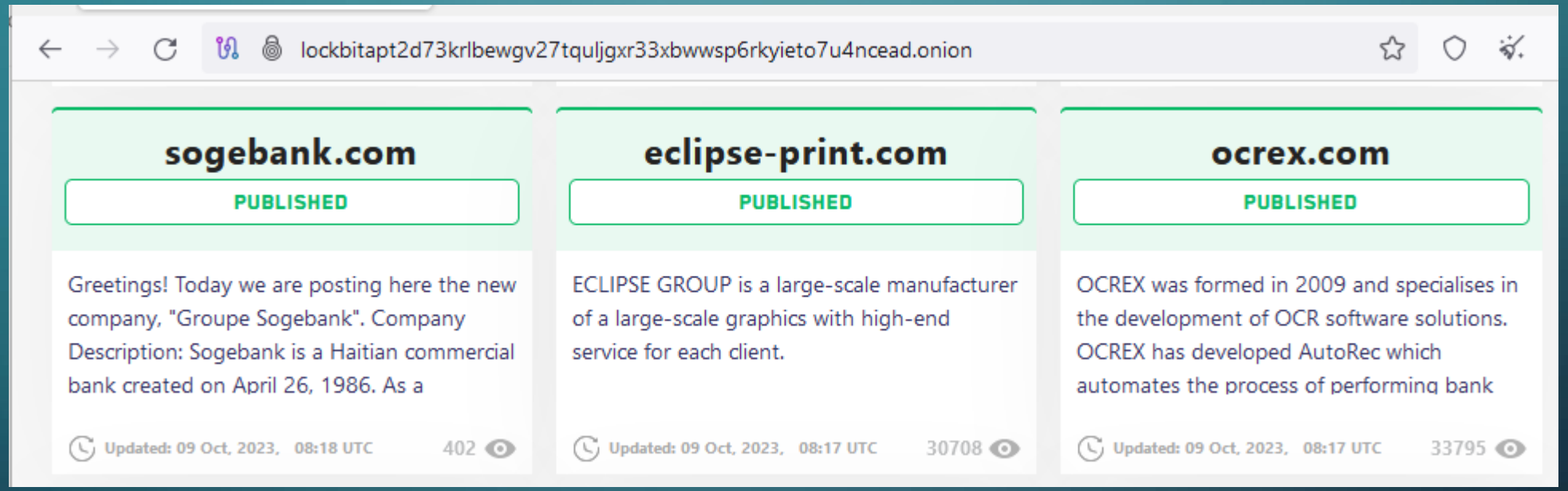
ATAQUES DE RANSOMWARE - APÓS

- 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

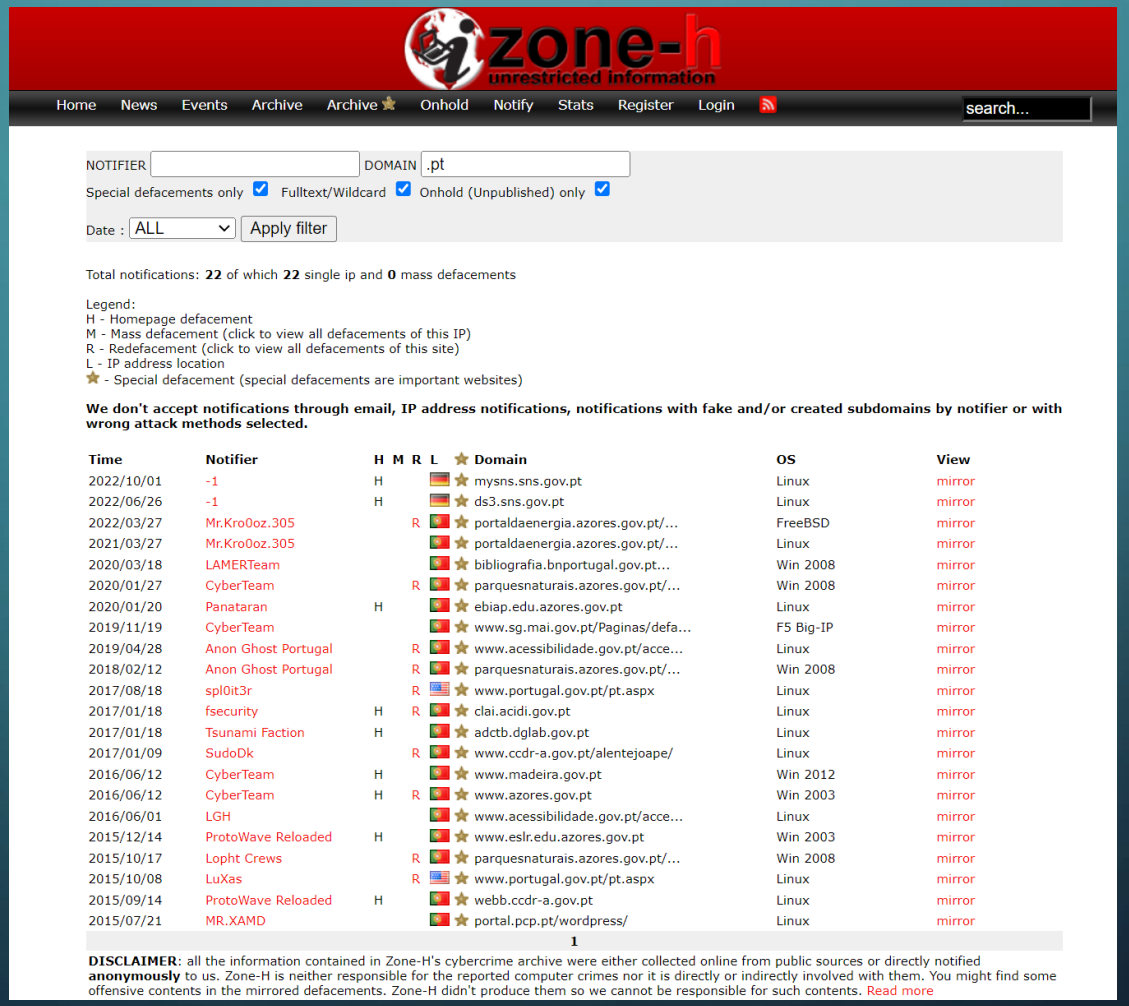


ATAQUES DE DEFACEMENT

- 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



zone-h
unrestricted information

Home | News | Events | Archive | Archive | Onhold | Notify | Stats | Register | Login | search...

NOTIFIER [ ] DOMAIN [.pt]
Special defacements only [x] Fulltext/Wildcard [x] Onhold (Unpublished) only [x]
Date : [ALL] [Apply filter]

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

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--b04fcdb6

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 envolvera-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 entreajuda". A Tomás Pedroso foi-lhe diagnosticado défice de atenção e hiperatividade e dificuldades em se socializar.

Trabalhadores das escolas estão esta segunda feira em greve por aumentos salariais

Com quantos deputados se ganha uma eleição? (em Espanha ou em qualquer lado)

Novos radares: multas de velocidade que foram originadas por falha técnica vão ser arquivadas

PARTILHA DE INFORMAÇÃO ENTRE ORGANISMOS PÚBLICOS

OBRIGADO