# Availability, a luxury or a right? DACYS TP3

Nuno Peralta

Nsp@isep.ipp.pt

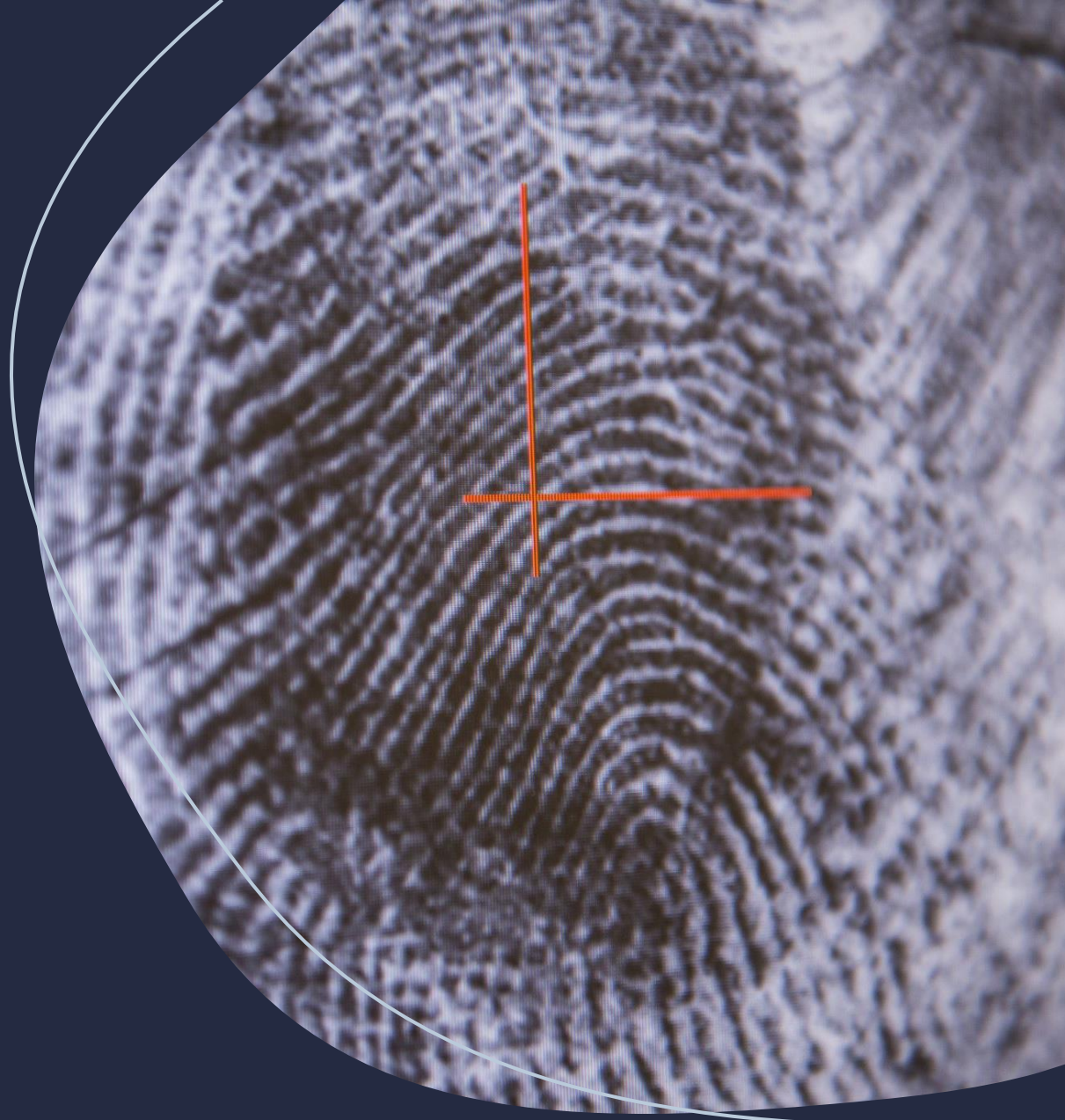
# The Triad

- Confidentiality
- Integrity
- Availability


https://kobalt.io/blogpost/confidentiality-integrity-and-availability-in-cyber-security/

# Confidentiality

- When data accessibility is limited, you significantly lower the chances of having information being leaked accidentally or intentionally.
- Examples of confidentiality risks include data breaches caused by criminals, insiders inappropriately accessing and/or sharing information, accidental distribution of sensitive information to too wide of an audience.

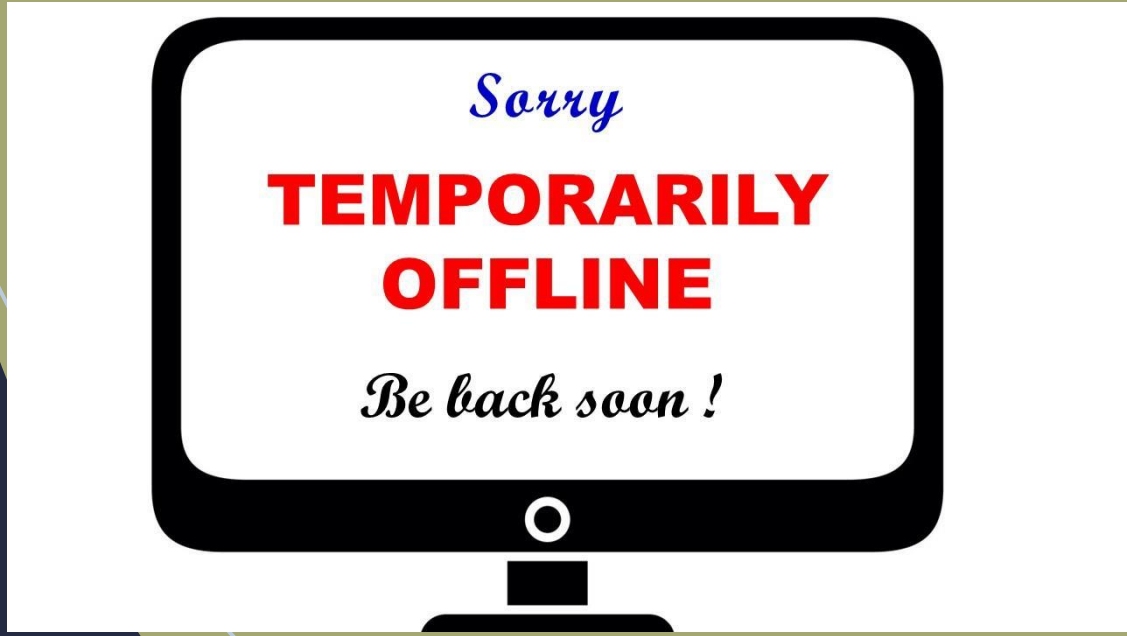


# Integrity

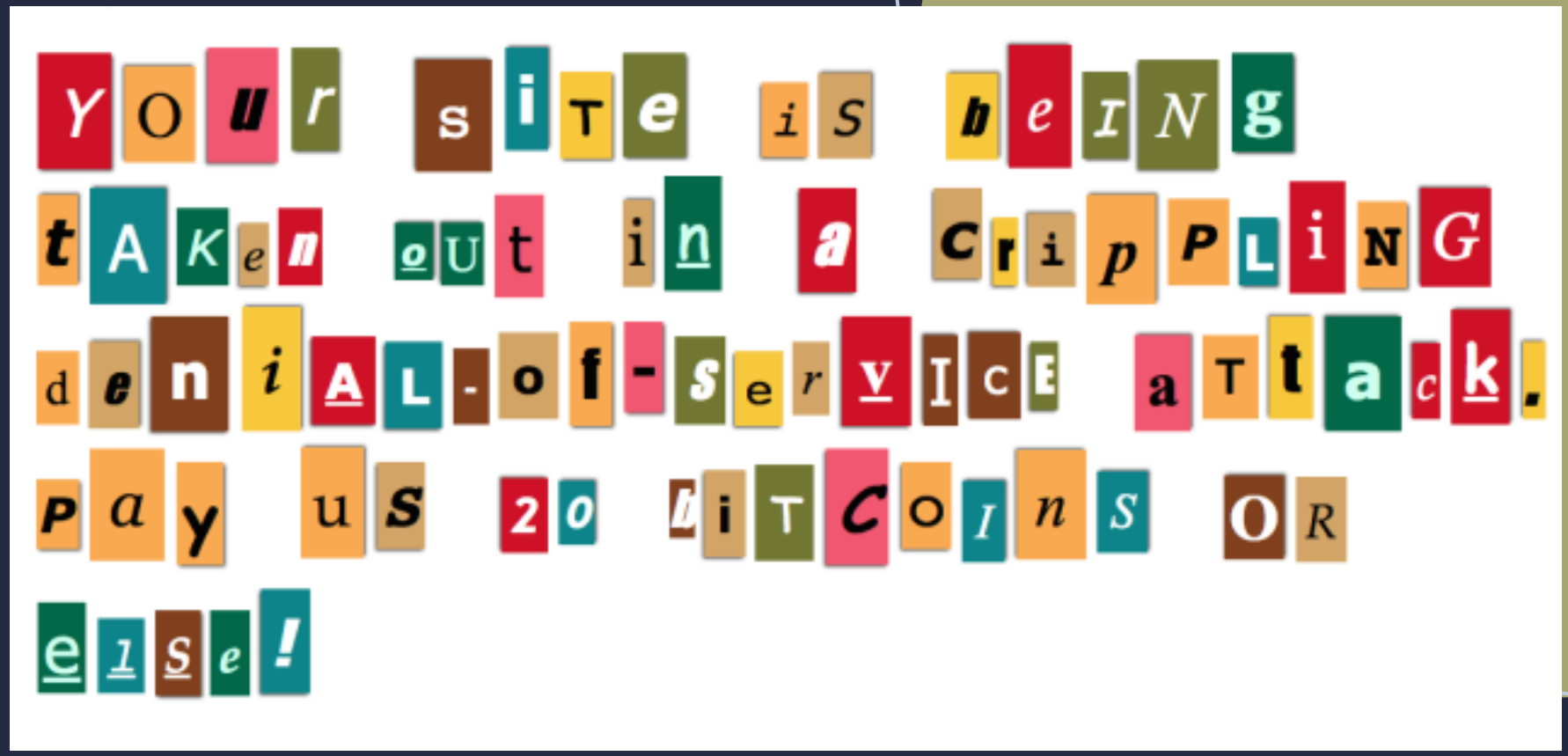
Integrity means that data or information in your system is maintained so that it is not modified or deleted by unauthorized parties.

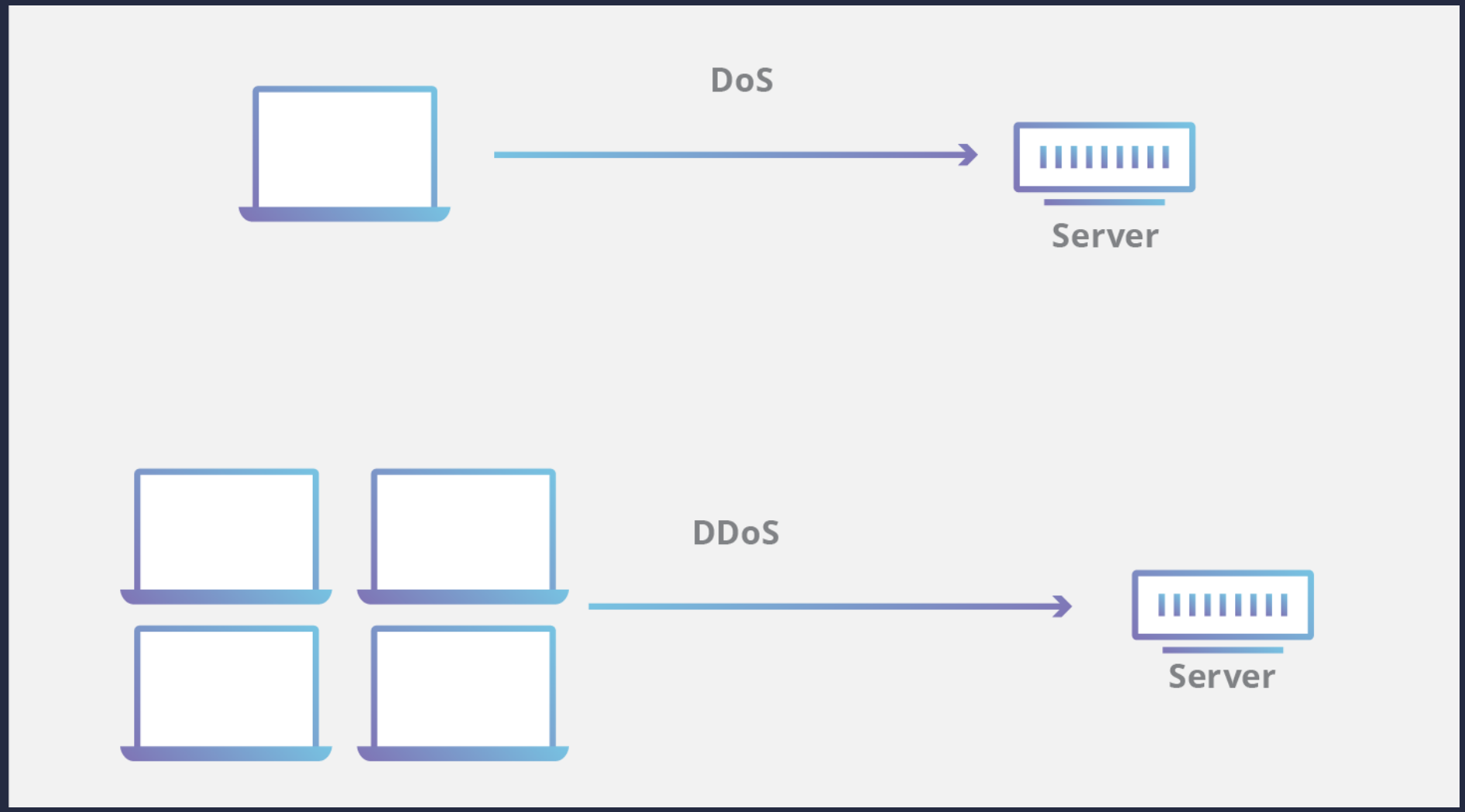
# Availability

- The final component of the CIA Triad is availability. It means that systems and data are available to individuals when they need it under any circumstances, including power outages or natural disasters. Without availability, even if you have met the other two requirements of the CIA Triad, your business can be negatively impacted.



# Importância da disponibilidade?




DoS
Server
DDoS
Server

# Vetores de amplificação

Volumetric DDos Attack:

- UDP Flood attacks
- CharGEN Flood
- ICMP (Ping) Flood
- ICMP Fragmentation Flood
- Misused application attack

Protocol:

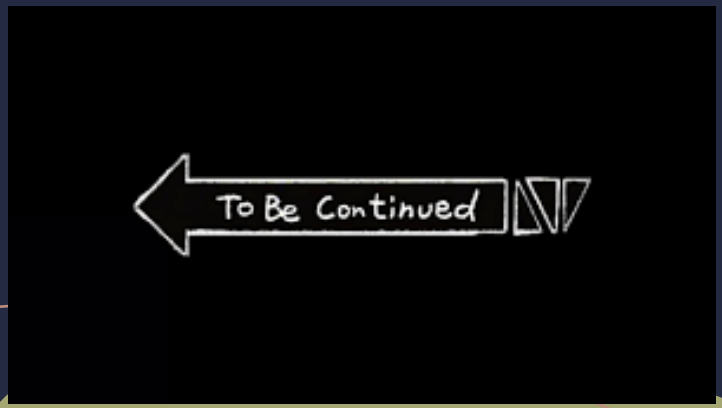
- IP Null attack
- TCP Flood attacks
- Session attack
- Slowloris
- Ping of Death
- Smurf attack
- Fraggle attack
- Low Orbit Ion Cannon (LOIC)
- High Orbit Ion Cannon (HOIC)

Application:

- HTTP Floods
- ReDoS

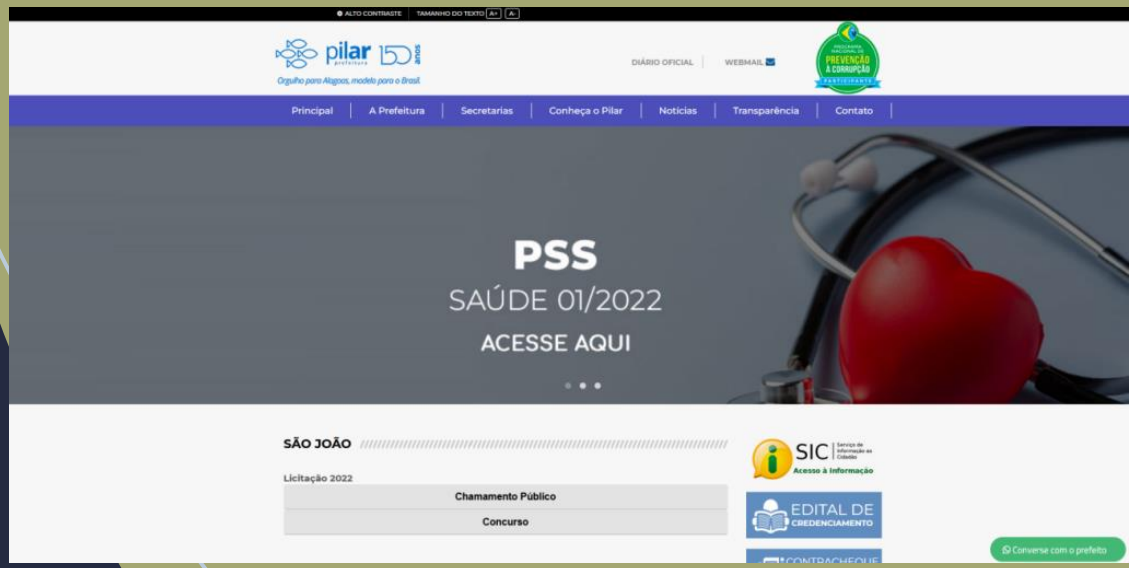
Excepcionais:

- Multi-vector attacks
- Advanced persistent DoS (APDoS)



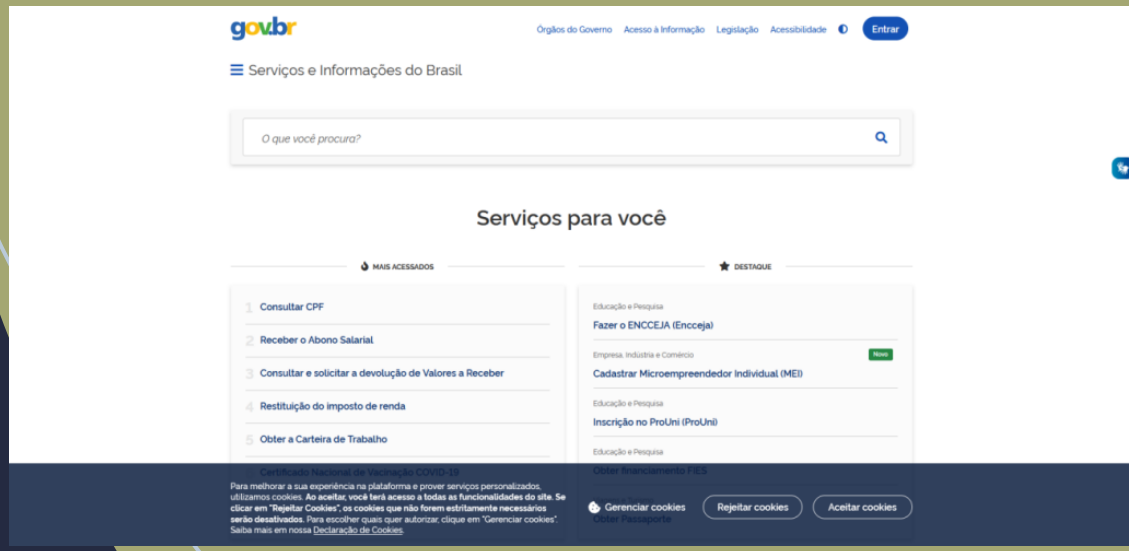
# Pilar City Hall (BR)

- At 9:10:20 AM, July 31 (Note: all time in this article refers to the Beijing Time), a reflection DDoS attack against the Brazilian government website Pilar City Hall (pilar.al.gov.br) was detected. In addition, there were another 15 websites of city halls in Brazil hit by massive DDoS attacks, too.



# Gov.br

At 13:08:38 on August 29, a DDoS reflection attack against the website of the Brazilian federal government was detected.



# A vista geral:

| Industry | Domain name | Start time of attack |
|---|---|---|
| Government | amtt.pontagrossa.pr.gov.br | 2022/7/10 5:21 |
| | www.sefanet.pr.gov.br | 2022/7/9 5:42 |
| | www.policiacivil.sp.gov.br | 2022/8/12 5:41 |
| | www.gov.br | 2022/8/29 13:08 |
| Education | ead.senarms.org.br | 2022/8/10 4:17 |
| | www.matriculaonline.sed.sc.gov.br | 2022/7/17 18:12 |
| Critical Infrastructure | itaipu.gov.br | 2022/7/9 4:14 |
| | neorede.com.br | 2022/7/31 9:45 |
| News Portal | g1.globo.com | 2022/7/15 6:17 |

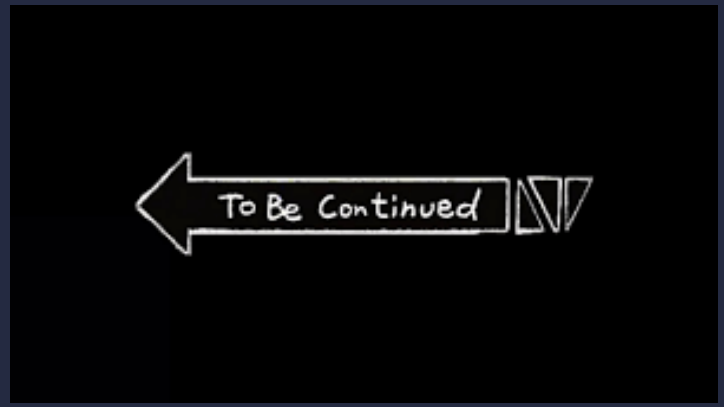
# Carpet-bombing Attacks

"Attackers used to target a single target IP with different attack methods in an attempt to evade protection polices. Unlike the previous attacks, carpet-bombing attacks are launched mostly using a common attack method that remians unchanged during the attack, but the traffic size on each IP address is too small to reach the cleaning threshold of the DDoS Defense system."

https://nsfocusglobal.com/large-scale-ddos-attacks-target-many-critical-industries-as-election-approaches-in-brazil/

# Como mitagar?

Real-time packet analysis
DDoS defense system (DDS)
Web application firewall
Rate limiting
Anomaly detection
Rerouting and scrubbing



# Dúvidas?