Cyber Minutes Weekly

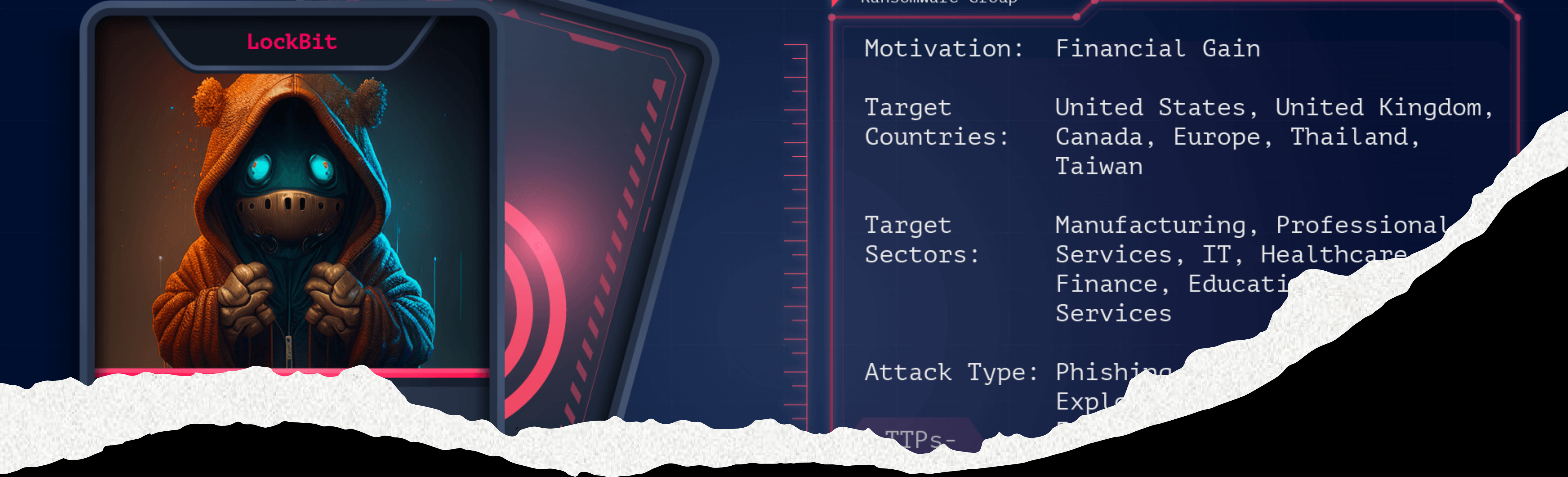
“Held for Ransom"

THE WORLD NEWS
$1.00
Since 1883
YOUR NUMBER ONE SOURCE FOR HEADLINES
CYBER ATTACK
24,000 FILES STOLEN IN LATEST ATTACK
IMPACT OF ATTACKS REACHING INTO THE ECONOMY
DEFENSE DE

11-15-2023 | Jonathan Montoya

LockBit

- Operation functions as a Ransomware-as-a-Service (RaaS)
- Charges a subscription fee, upfront payments, or a portion of the profit
- Most active in 2022 and 2023
- Over 1,700 attacks since 2020 in the U.S.
- Active since late 2019



Ransomware Group

Motivation: Financial Gain

Target Countries: United States, United Kingdom, Canada, Europe, Thailand, Taiwan

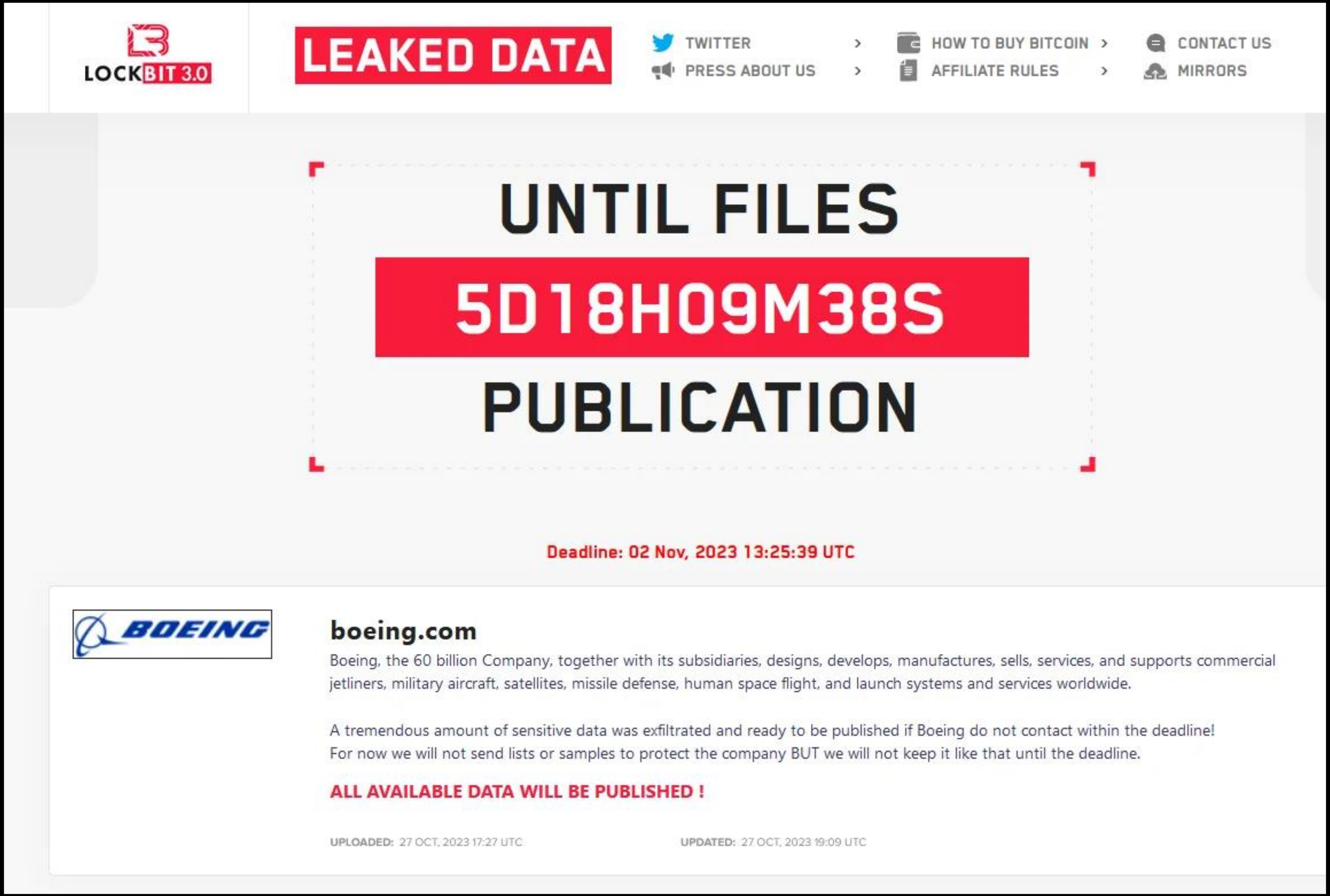
Target Sectors: Manufacturing, Professional Services, IT, Healthcare, Finance, Educati Services

Attack Type: Phishi Expl

TTPs-

Ran$omware

- "Dark Corporations" like DarkSide, Clop, Dark Angels Team, and many more.
- Major companies hit including MGM, Boeing, Johnson Controls, Sony, etc.
- LockBit has collected over 100M in U.S. ransom payments since 2020
- Targets Windows, Linux and now MacOS
- LockBit 3.0 builder leaked in late 2022



UNTIL FILES

5D18H09M38S

PUBLICATION

Deadline: 02 Nov, 2023 13:25:39 UTC

boeing.com

Boeing, the 60 billion Company, together with its subsidiaries, designs, develops, manufactures, sells, services, and supports commercial jetliners, military aircraft, satellites, missile defense, human space flight, and launch systems and services worldwide.

A tremendous amount of sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline!
For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline.

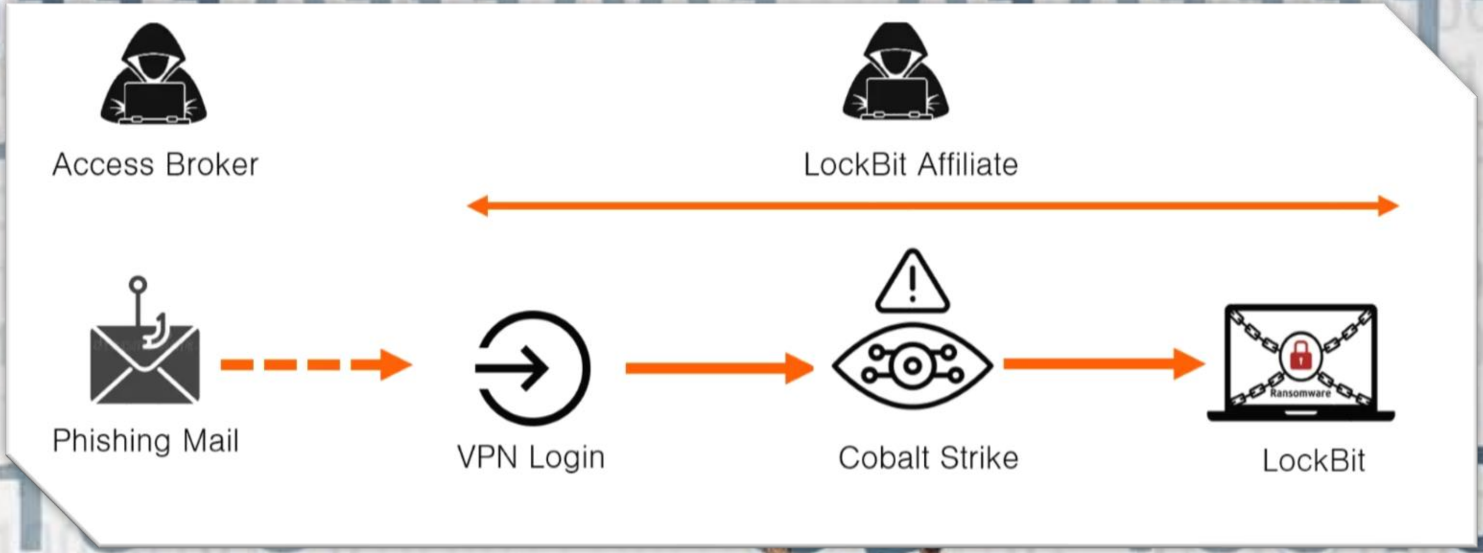
ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 27 OCT, 2023 17:27 UTC

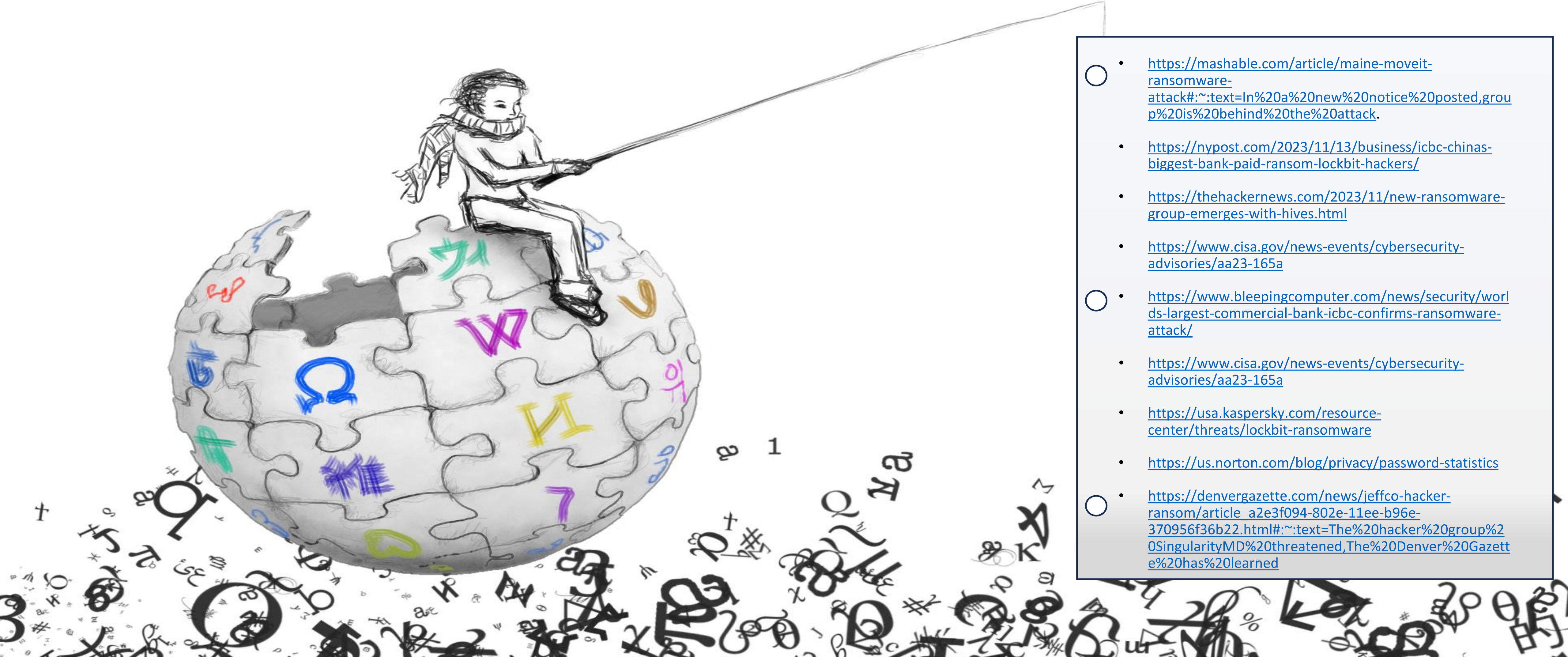
UPDATED: 27 OCT, 2023 19:09 UTC

How do we protect ourselves? 🔒

- Strong Passwords
- Multi-factor authentication
- Never blindly click a link
- Use trusted anti-virus
- Keep all systems updated
- Regularly back up and store off-site



Sources



- https://mashable.com/article/maine-moveit-ransomware-attack#:~:text=In%20a%20new%20notice%20posted,group%20is%20behind%20the%20attack.
- https://nypost.com/2023/11/13/business/icbc-chinas-biggest-bank-paid-ransom-lockbit-hackers/
- https://thehackernews.com/2023/11/new-ransomware-group-emerges-with-hives.html
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
- https://www.bleepingcomputer.com/news/security/worlds-largest-commercial-bank-icbc-confirms-ransomware-attack/
- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a
- https://usa.kaspersky.com/resource-center/threats/lockbit-ransomware
- https://us.norton.com/blog/privacy/password-statistics
- https://denvergazette.com/news/jeffco-hacker-ransom/article_a2e3f094-802e-11ee-b96e-370956f36b22.html#:~:text=The%20hacker%20group%20SingularityMD%20threatened,The%20Denver%20Gazette%20has%20learned