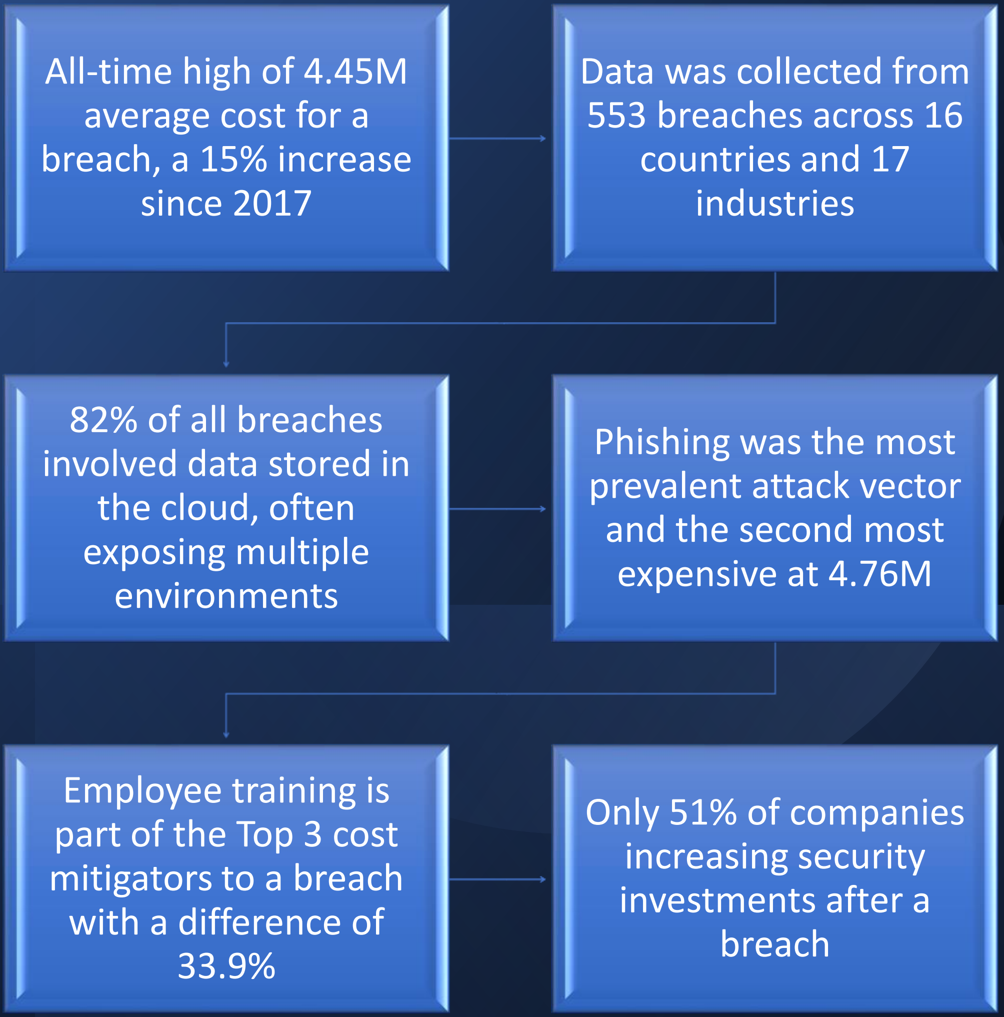
# Cyber Minutes

*"A Year in Review "*

*12-27-2023 | Jonathan Montoya*

# IBM Cost of Data Breach Report



All-time high of 4.45M average cost for a breach, a 15% increase since 2017

Data was collected from 553 breaches across 16 countries and 17 industries

82% of all breaches involved data stored in the cloud, often exposing multiple environments

Phishing was the most prevalent attack vector and the second most expensive at 4.76M

Employee training is part of the Top 3 cost mitigators to a breach with a difference of 33.9%

Only 51% of companies increasing security investments after a breach

## Cost of a data breach by industry

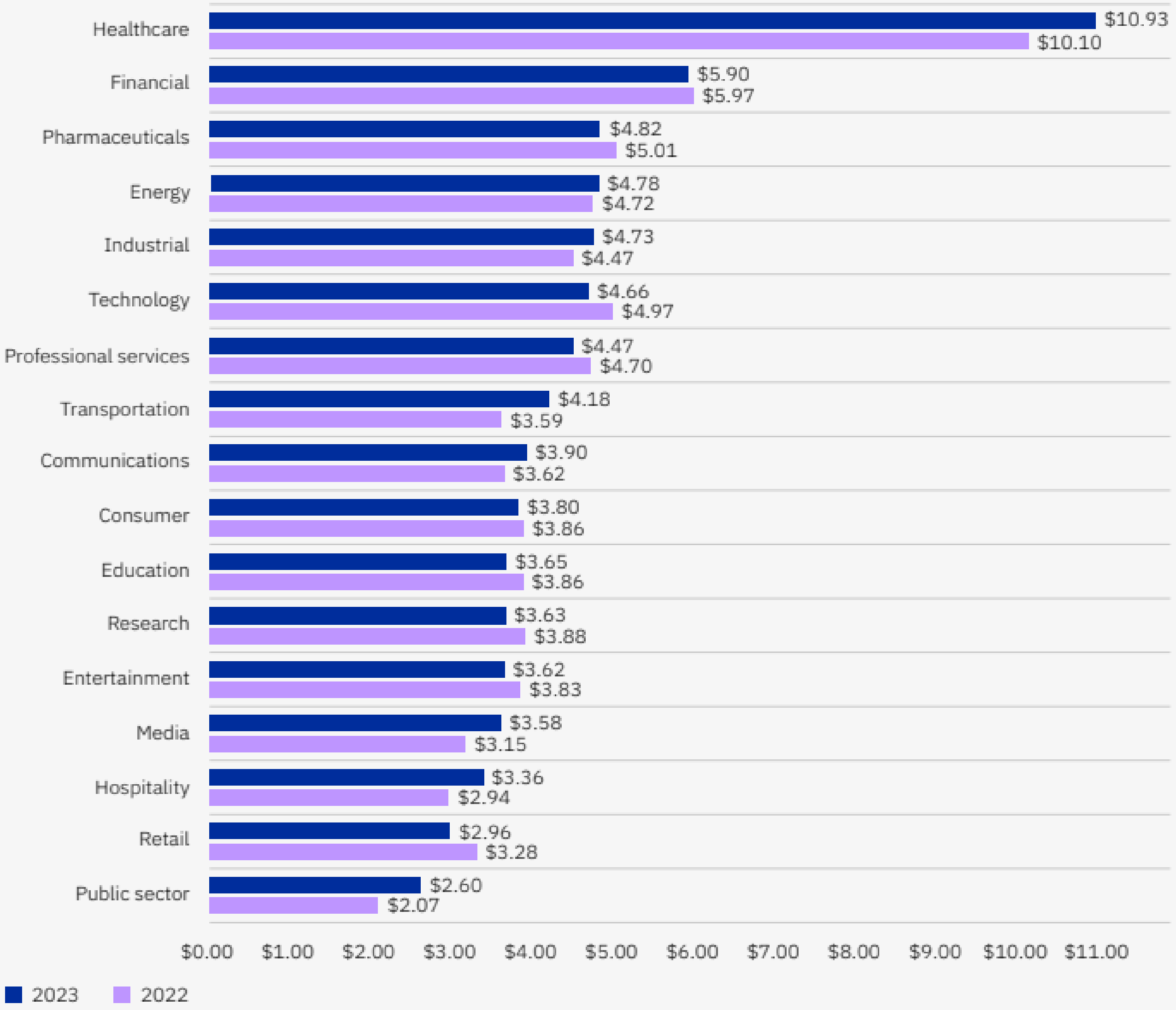
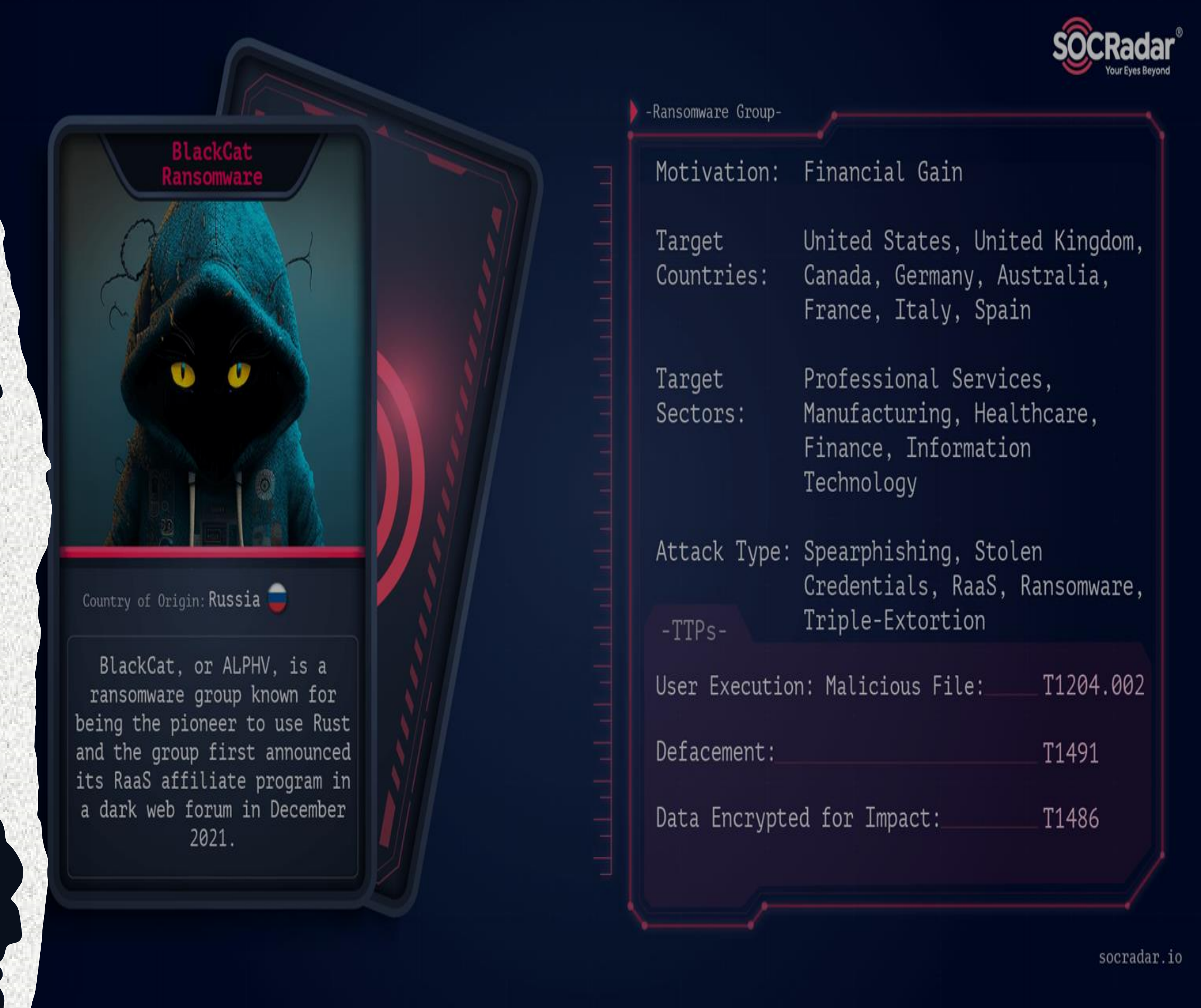


Figure 4. Measured in USD millions

# Decrypted

- FBI released a free decryption tool for the BlackCat Ransomware
- This decryption tool allows over 500 victims to recover their filed locked by the malware
- BackCat RaaS has breached the networks of over 1,000 victims and has illegally earned close to 300M as of mid-2023
- BlackCat representative told vx-underground reporter that law enforcement only had access to an old key
- Other RaaS groups like LockBit were quick to capitalize on the news by offering those who were still in "negotiations" their infrastructure



BlackCat Ransomware

Country of Origin: Russia

BlackCat, or ALPHV, is a ransomware group known for being the pioneer to use Rust and the group first announced its RaaS affiliate program in a dark web forum in December 2021.

-Ransomware Group-

Motivation: Financial Gain

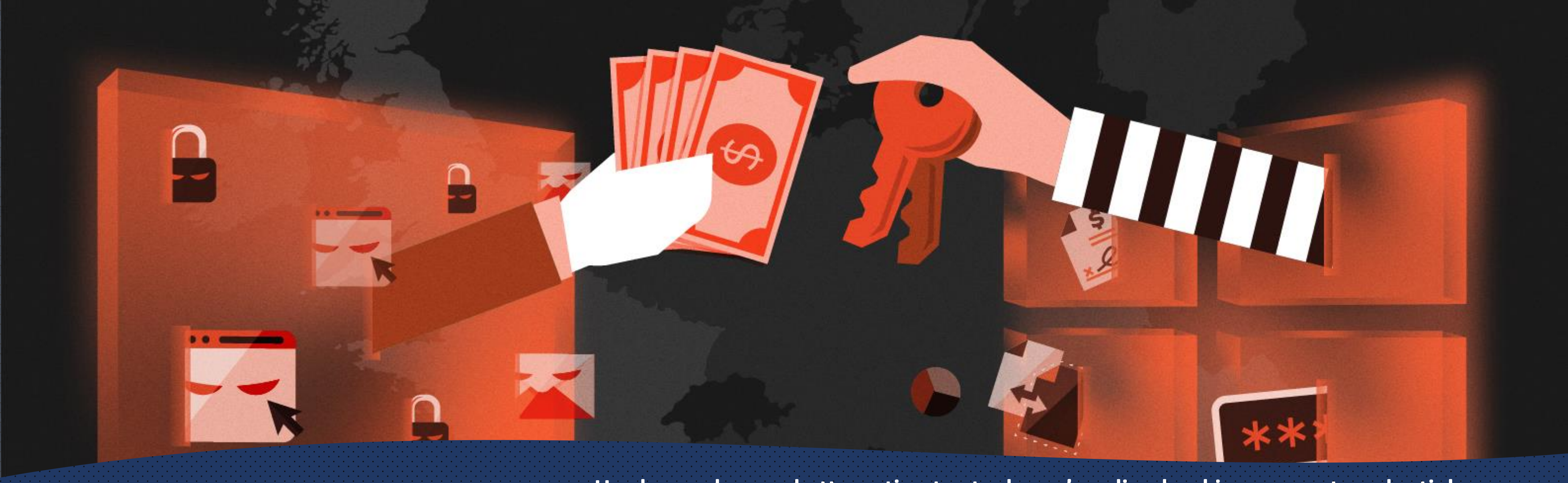
Target Countries: United States, United Kingdom, Canada, Germany, Australia, France, Italy, Spain

Target Sectors: Professional Services, Manufacturing, Healthcare, Finance, Information Technology

Attack Type: Spearphishing, Stolen Credentials, RaaS, Ransomware, Triple-Extortion

-TTPs-

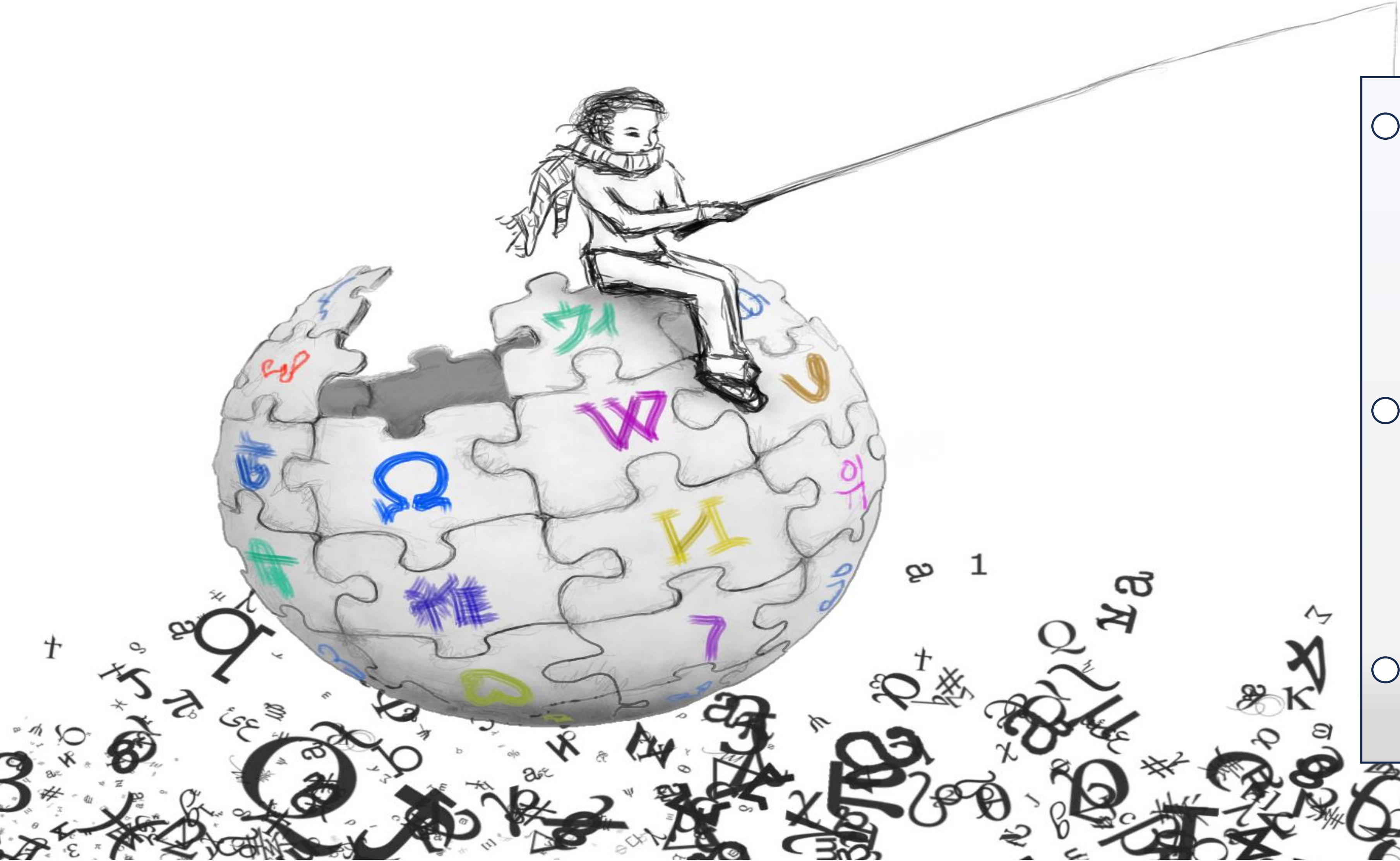
| | |
|---|---|
| User Execution: Malicious File: | T1204.002 |
| Defacement: | T1491 |
| Data Encrypted for Impact: | T1486 |



# JavaScript Malware Infection

- Has been observed attempting to steal user's online banking account credentials
- Estimated 50,00 infected user sessions across the globe
- Web injection module delivered likely through phishing emails
- Described as highly dynamic allowing it to adjust its flow of data to the C2 server or even erase traces of itself. This type of advanced code could possibly delay any immediate deployment, avoiding detection upon download
- Will even display an error message after the user enters their credentials, saying something like this page is unavailable for the next 12 hours. This would give the attackers a window of opportunity to have free reign on the account

# Sources



- https://thehackernews.com/2023/12/fbi-takes-down-blackcat-ransomware.html
- https://www.proofpoint.com/us/blog/security-awareness-training/2023-state-of-the-phish-findings-sneak-peek
- https://www.microsoft.com/en-us/security/blog/2023/01/25/microsoft-security-reaches-another-milestone-comprehensive-customer-centric-solutions-drive-results/
- https://www.varonis.com/blog/data-breach-statistics
- https://www.ibm.com/reports/data-breach
- https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
- https://thehackernews.com/2023/12/new-javascript-malware-targeted-50000.html