Galvez, Hance Henley S. BSIT4-1AA 10/22/2023

Information Assurance and Security (Data Privacy)  
03 Laboratory Exercise 2

1. **Title and Link to the Article:**

Title: 'Philippines 2nd most attacked by web threats worldwide last year'

Link: Read the full article here: <https://www.philstar.com/headlines/2023/03/15/2251710/philippines-2nd-most-attacked-web-threats-worldwide-last-year>

1. **Article Summary:**

According to a report from the Kaspersky Security Network (KSN), the Philippines was the second most-attacked country by web threats worldwide in the previous year. The data, collected from January to December of the same year, revealed that the Philippines moved up two places, ranking as the second most attacked. Mongolia topped the global ranking with 51.1 percent of recorded attacks, followed closely by the Philippines at 49.8 percent.

The report highlights that these rankings are based on the number of web-based cyberthreats detected and blocked by Kaspersky's security products. It also emphasizes that a single device can be a target for multiple cyberattacks.

The nature of the attacks is not explicitly mentioned in the summary, but considering that the Philippines was targeted by "web threats," it can be inferred that these are active attacks. Active attacks involve malicious actors actively trying to compromise systems, which aligns with the context of web threats.

1. **Recommendations to Prevent the Identified Attack:**

The article does not provide specific recommendations for preventing these attacks. However, based on general cybersecurity best practices, here are some measures that can help prevent and mitigate web-based attacks:

* **Use Reliable Security Software:** Employ reputable antivirus and anti-malware software to detect and block web threats in real-time.
* **Regular Software Updates:** Keep all software, including operating systems and applications, up to date to patch known vulnerabilities.
* **User Training:** Educate users, both individuals and organizations, about safe web browsing practices, recognizing phishing attempts, and avoiding suspicious links and downloads.
* **Strong Passwords:** Encourage the use of strong and unique passwords, and consider using a password manager to help users keep track of their credentials.
* **Access Control:** Implement strict access controls and least privilege principles to restrict access to sensitive data and resources
* **Data Encryption:** Encrypt sensitive data in transit and at rest to make it difficult for attackers to steal or manipulate information.
* **Incident Response Plan:** Develop an incident response plan to quickly identify and respond to security incidents, minimizing their impact.
* **Regular Backups:** Regularly back up critical data to secure, off-site locations to mitigate data loss in the event of a breach.
* **Security Awareness:** Promote a culture of cybersecurity awareness within organizations and among individuals to foster vigilance against web threats.