The Eye, CSEA

Notice w.r.t Recent Cyber Attacks in India

April 10, 2023

To all members of The Eye

Anonymous is a decentralized group of activists and hackers who are known for their online activism, particularly through the use of DDOS attacks and information leaks. The group has no central leadership, and its members are spread out across the world.

#OpSudan is a campaign launched by Anonymous Sudan, a group of politically motivated hackers from Sudan. The campaign involves DDOS attacks against various targets, including government institutions and companies. #OpSudan's attacks on Indian institutions, such as major financial and e-commerce websites, could potentially disrupt critical infrastructure and cause economic damage. OpSudan launched a cyber attack on India's major institutions and online shopping websites on the evening of April 8, 2023. On April 9, 2023, a few Indian websites such as SBI, Bank of India, IRCTC, AIIMS, and Income Tax website were also targeted with a DDoS attack.

It is important for individuals to **practice good cyber hygiene**, such as using strong passwords, avoiding suspicious links and emails, and keeping their software up-to-date. We request all members to take up the **ISEA Certified Cyber-Hygiene Practitioner certification at https://www.infosecawareness.in/chpquiz**

The B**ug Bounty Research Team will be performing ethical penetration testing, vulnerability assessment, and responsible vulnerability disclosure on critical infrastructure**, which will be helpful for improving the security of the critical infrastructure. By identifying vulnerabilities and weaknesses in the systems and networks, we can provide valuable information to the organizations responsible for securing the critical infrastructure. The organizations can then use this information to prioritize and address security issues, potentially preventing cyberattacks.

In addition to ethical penetration testing and vulnerability assessment activities in the club, we take several other countermeasures to protect against cyber threats. These include:

1. Conducting **regular security audits and risk assessments** to identify and mitigate potential risks – done by **the Bug Bounty Research Team, with assistance from Intel and OSINT team**.
2. Developing and implementing **an incident response plan** and developing intelligent and innovative incident detection systems to respond quickly and effectively to cyber-attacks – will be worked-on by **the R&D Team**, alongwith proper platform development for the same by **the Oculus UI Team**.
3. Providing **regular security awareness training** to students and employees of organizations to educate them on cybersecurity best practices and the potential risks of cyber-attacks – webinars and other such awareness drives to be planned by **the Media Team**, **the Training Team** and **the YouTube Team**.

Overall, a multi-faceted approach to cybersecurity is essential to protect critical infrastructure from cyber threats. Ethical penetration testing, vulnerability assessment, and responsible vulnerability disclosure can be valuable components of this approach, but they should be complemented by other measures to ensure the security and resilience of critical infrastructure.

Aaditya Rengarajan,
The Eye, CSEA.

www.cseatheeye.com
E-mail: 21Z202@psgtech.ac.in