SYLHET GANG-SG hacktivist group

By: Mohamed Galal Hashem

Source:

1- SOCRadar Report (link to report)

2- group telegram (Link to channel)

3- cloudsek Report (link to report)

4- searching in social media by using hashtag #Sylhet Gang-SG and their account in x (P@kistanCyberForce [@Cyb67723])

5- some article about India-Pakistan war (article)

6- cloudsek Report (Link to report)

Introduction to SYLHET GANG-SG:

- SYLHET GANG-SG is identified as a hacktivist group originating from Bangladesh, operating with distinct politically motivated objectives.
- SYLHET GANG-SG has declared allegiance to the KillNet 2.0 hacker collective.
- SYLHET GANG-SG is known for its collaborations with other hacktivist entities, such as DieNet, and its activities are frequently associated with larger Pakistan-aligned hacktivist campaigns.
- The group's primary methods of operation include Distributed Denial of Service (DDoS) attacks and website defacements.
- More recently, the group's activities have strongly focused on Indian digital infrastructure, framed within the context of geopolitical tensions between India and Pakistan.
- A primary motivation initially cited for their activities is "threats against allies of Israel" which positions the group within the broader pro-Palestinian hacktivist movement.
- Primary Platforms Used for Operations and Claims: Telegram, X (formerly Twitter), Dark Web.

SYLHET GANG-SG attack methods:

- SYLHET GANG-SG employs a range of attack methods, primarily focusing on those that yield immediate, visible, and often symbolic results.
- Common Attack Methods Employed:
    - Distributed Denial of Service (DDoS) Attacks
    - SYLHET GANG-SG has allegedly defaced Indian websites, often to display political messages supporting Pakistan.
    - The group frequently claims to have exfiltrated large volumes of sensitive data from targeted entities.

Overview of Typical Target Sectors:

Their target sectors include:

- Government: This is a prominent target sector, encompassing central government portals and administrative websites
- Educational Institutions: Universities and colleges are frequently targeted.
- News Media Outlets: These are targeted, likely for their public visibility and ability to disseminate information

Assessing Group Reliability and Actual Impact:

- A critical assessment of SYLHET GANG-SG's activities reveals a consistent pattern of exaggerated claims and minimal actual impact, highlighting the group's reliance on psychological warfare over technical prowess.
- Cybersecurity firm CloudSEK has consistently found that the claims made by SYLHET GANG-SG and other similar hacktivist groups were "largely exaggerated or entirely fabricated".
- The overall actual impact of SYLHET GANG-SG's activities is consistently assessed as "minimal" by cybersecurity experts, including CloudSEK. Their actions are primarily "symbolic," designed for visibility and psychological effect rather than causing deep system compromise or significant, lasting disruption.