

4<sup>th</sup> August 2023

## SITUATIONAL ALERT ON CYBER THREATS

In a response to a declaration made by some religious and ideologically motivated underground hacker groups on 31<sup>st</sup> July to launch as they mentioned a storm of cyber-attacks against Bangladesh cyberspace on next 15<sup>th</sup> August, Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is releasing this alert to warn critical information infrastructures (CII), banks and financial institutions, health care and all sorts of government and private organizations of the possible conducted cyber-attacks by the groups that may disrupt IT operations and businesses. All organizations are advised to be on alert for small to medium-scale cyber-attacks originating from the subject hacktivist groups and to take the required precautions to protect their infrastructures.



### Groups' background and their operations

These groups claim to be hacktivist groups and have been targeting organizations from Pakistan, and Bangladesh. In our recent research, we identified several groups with the same motivation. They have been incessantly conducting frequent cyber-attacks against organizations in Bangladesh affecting its operations and businesses. The groups' primary attack tactics include:

- *Distributed Denial-of-Service (DDoS) attacks*
- *Website defacements, compromising the website*
- *Using malicious PHP shells as a backdoor to drop payloads*



*Top targeted Organization Type:*

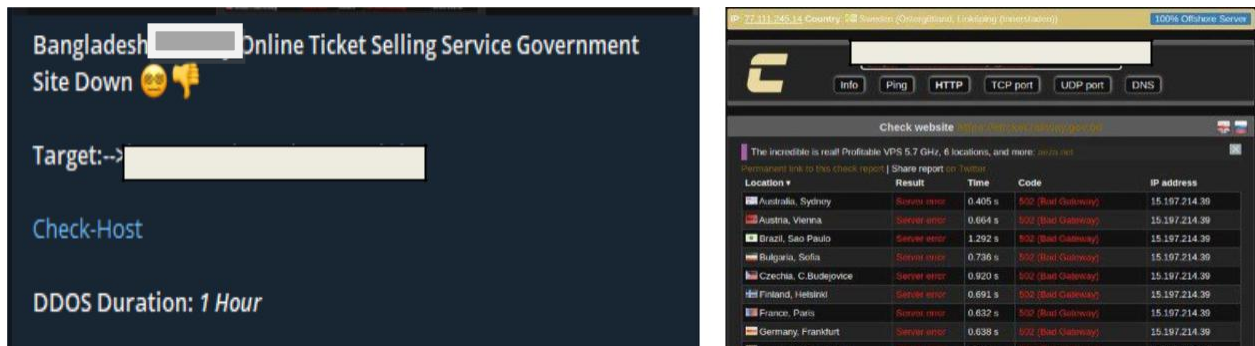
- *Gov't & Military*
- *Law Enforcement Agencies*
- *Banking and NBF*
- *Pharmaceuticals*
- *Retail and Industrial Organizations*
- *Energy and education sectors*

## Recent Notable Activities Targeting Bangladesh

1. On August 01, 2023, a hacker group claimed a cyber-attack on Payment Gateway in Bangladesh and Law enforcement & banking organizations.



2. On July 03, 2023, a hacker group claimed a DDoS attack on Bangladeshi transportation service for 1 hour making the website unavailable for the mentioned time.



3. On June 27, 2023, a hacker group defaced the website of a Bangladesh government college and shared a web archive supporting their claims.



4. On June 24, 2023, a hacker group defaced the website of a Bangladesh health organization and shared a web archive supporting their claims.

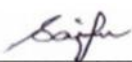


5. On June 21, 2023, the group claimed a DDoS attack on the website of Bangladeshi military organizations.

6. On June 20, 2023, the group claimed to compromise Bangladesh's state-owned investment company, and exfiltrated data of over 100,000 investors and investment applicants. The threat group shared a single screenshot as proof of compromise and planned to release the data after successful exfiltration.

➤ **All organizations in Bangladesh are requested to take the following measures to ensure their infrastructures' security:**

- Ensure strict network and user activity monitoring 24/7, especially during non-office hours, and watch out for any indication of data exfiltration.
- Ensure implementing load balancer solutions to ensure that no single server is overwhelmed during an attack.
- Deploy a Web Application Firewall to analyze incoming HTTP/HTTPS traffic and filter out malicious requests and traffic patterns commonly associated with DDoS attacks.
- Ensure vital services such as DNS, NTP as well as network middleboxes are securely configured and are not exposed on the internet.
- Validate and sanitize all user input to prevent malicious code injection (e.g., SQL injection, Cross-Site Scripting) that could lead to web defacement.
- Perform regular backups of your website's content and database. In the event of defacement, having up-to-date backups enables you to restore your website quickly.
- Enforce HTTPS on your website with SSL/TLS encryption. This helps protect data during transmission and prevents attackers from tampering with website content in transit.
- Keep all web server software, content management systems (CMS), plugins, and other software components up-to-date with the latest security patches.
- Configure and harden web application as per OWASP guideline (<https://owasp.org/www-project-web-security-testing-guide/v41/>)
- Report or inform BGD e-GOV CIRT regarding the detection of IOCs and/ or any suspicious activities you observe within your environment, to work in collaboration through <https://www.cirt.gov.bd/incident-reporting/> or [cti@cirt.gov.bd](mailto:cti@cirt.gov.bd)



Engr. Mohammad Saiful Alam Khan  
Project Director  
BGD e-GOV CIRT