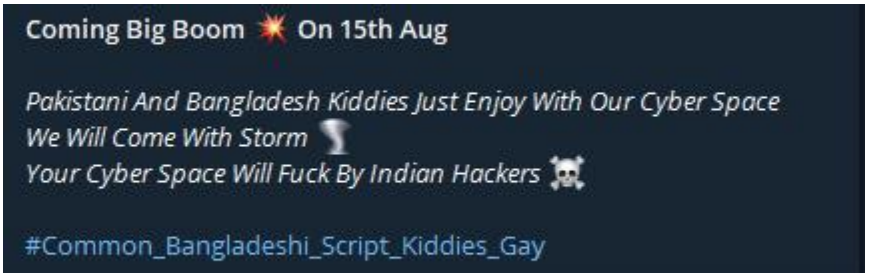
4th August 2023

SITUATIONAL ALERT ON CYBER THREATS

In a response to a declaration made by some religious and ideologically motivated underground hacker groups on 31st July to launch as they mentioned a storm of cyber-attacks against Bangladesh cyberspace on next 15th 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.



Coming Big Boom 💥 On 15th Aug

Pakistani And Bangladesh Kiddies Just Enjoy With Our Cyber Space
We Will Come With Storm 🌪
Your Cyber Space Will Fuck By Indian Hackers ☠️

#Common_Bangladeshi_Script_Kiddies_Gay

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:

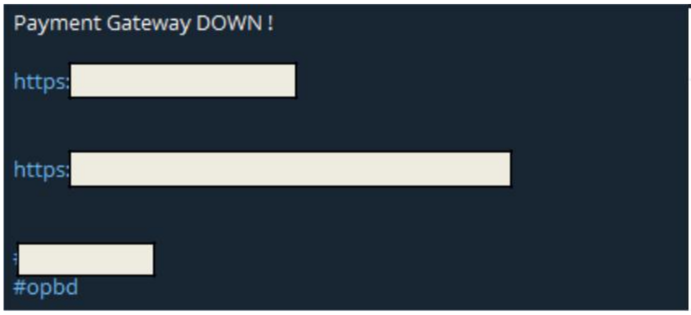
- *Distributed Denial-of-Service (DDoS) attacks*
- *Website defacements, compromising the website*
- *Using malicious PHP shells as a backdoor to drop payloads*

➢ *Top targeted Organization Type:*

  - *Gov’t & Military*
  - *Law Enforcement Agencies*
  - *Banking and NBFI*
  - *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.

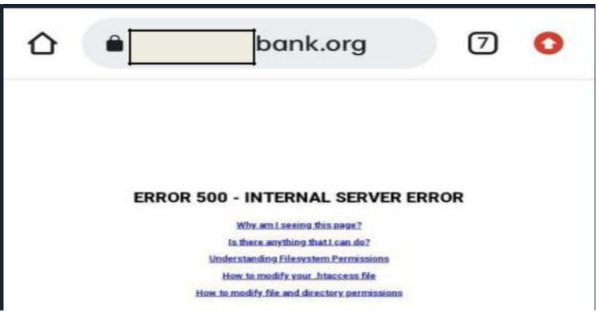


Payment Gateway DOWN !

https:[redacted]

https:[redacted]

:[redacted]
#opbd

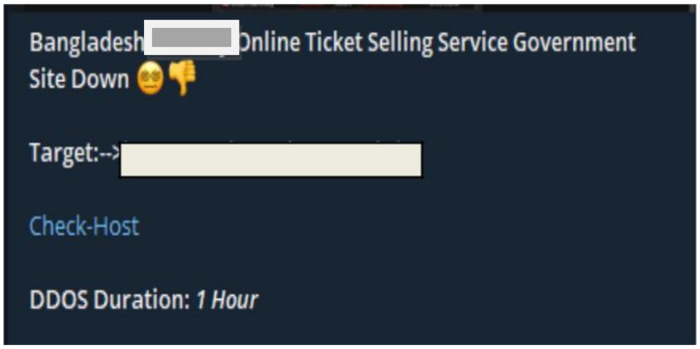


[redacted]bank.org

ERROR 500 - INTERNAL SERVER ERROR

Why am I seeing this page?
Is there anything that I can do?
Understanding Filesystem Permissions
How to modify your .htaccess file
How to modify file and directory permissions

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.

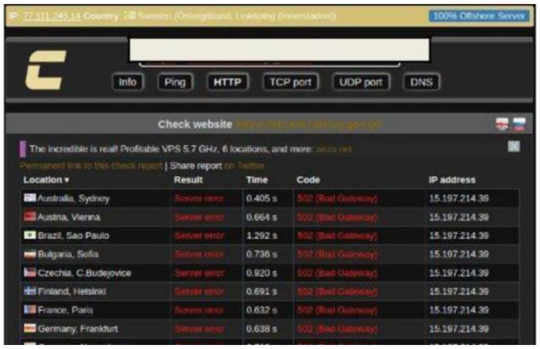


Bangladesh[redacted]Online Ticket Selling Service Government Site Down 😳👎

Target:-->[redacted]

Check-Host

DDOS Duration: *1 Hour*



IP: 77.111.245.14 Country: Sweden (Östergötland, Linköping (Innerstaden)) 100% Offshore Server

[redacted]

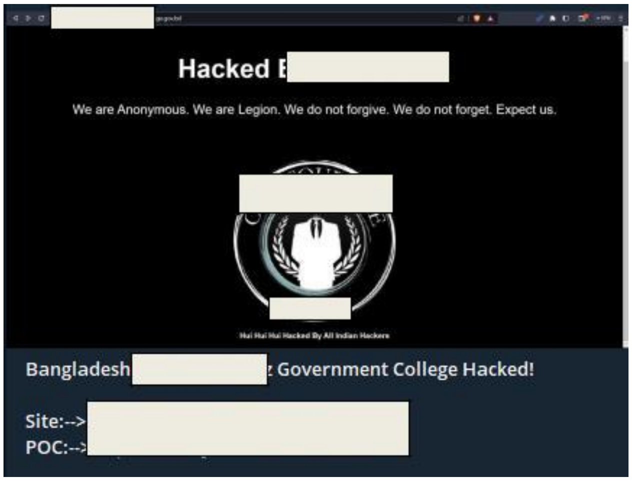
Check website [illegible]

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

Permanent link to this check report | Share report on Twitter

Location ▾	Result	Time	Code	IP address
Australia, Sydney	Server error	0.405 s	502 (Bad Gateway)	15.197.214.39
Austria, Vienna	Server error	0.664 s	502 (Bad Gateway)	15.197.214.39
Brazil, Sao Paulo	Server error	1.292 s	502 (Bad Gateway)	15.197.214.39
Bulgaria, Sofia	Server error	0.736 s	502 (Bad Gateway)	15.197.214.39
Czechia, C.Budejovice	Server error	0.920 s	502 (Bad Gateway)	15.197.214.39
Finland, Helsinki	Server error	0.691 s	502 (Bad Gateway)	15.197.214.39
France, Paris	Server error	0.632 s	502 (Bad Gateway)	15.197.214.39
Germany, Frankfurt	Server error	0.638 s	502 (Bad Gateway)	15.197.214.39

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



[redacted]

Hacked B[redacted]

We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.

[redacted]

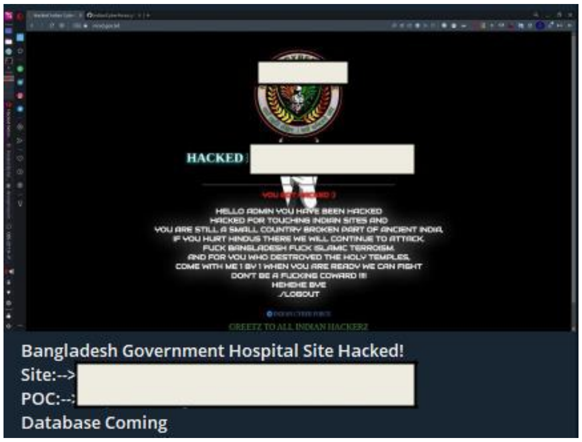
[redacted]

Hui Hui Hui Hacked By All Indian Hackers

Bangladesh[redacted]: Government College Hacked!

Site:-->[redacted]
POC:-->

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



[redacted]

HACKED [redacted]

YOU [illegible] :)

HELLO ADMIN YOU HAVE BEEN HACKED
HACKED FOR TOUCHING INDIAN SITES AND
YOU ARE STILL A SMALL COUNTRY BROKEN PART OF ANCIENT INDIA,
IF YOU HURT HINDUS THERE WE WILL CONTINUE TO ATTACK.
FUCK BANGLADESH FUCK ISLAMIC TERRORISM.
AND FOR YOU WHO DESTROYED THE HOLY TEMPLES,
COME WITH ME 1 BY 1 WHEN YOU ARE READY WE CAN FIGHT
DON'T BE A FUCKING COWARD !!!
HEHEHE BYE
./LOGOUT

INDIAN CYBER FORCE

GREETZ TO ALL INDIAN HACKERZ

Bangladesh Government Hospital Site Hacked!
Site:--> [redacted]
POC:--:
Database Coming

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://onwasp.onrg/www-pronject-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

Saiful

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