গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়
আইসিটি সেল
www.mocat.gov.bd

জরুরি

স্মারক নম্বর: ৩০.০০.০০০০.০২৩.৯৯.০০২.২১.৮১

তারিখ: ২৪ শ্রাবণ ১৪৩০
০৮ আগস্ট ২০২৩

বিষয়: **ডিজিটাল অবকাঠামো নিরাপদ রাখার লক্ষ্যে কার্যক্রম গ্রহণ প্রসংগে।**

সূত্র: বাংলাদেশ কম্পিউটার কাউন্সিল হতে প্রাপ্ত ই-মেইল, তারিখ: ০৮/০৮/২০২৩।

উপর্যুক্ত বিষয়ে বাংলাদেশ কম্পিউটার কাউন্সিল হতে প্রাপ্ত ই-মেইল এর পরিপ্রেক্ষিতে জানানো যাচ্ছে যে, একদল আন্ডারগ্রাউন্ড হ্যাকার গ্রুপ আগামী ১৫ আগস্ট ২০২৩ তারিখে বাংলাদেশের সাইবারস্পেসের বিরুদ্ধে একটি সিরিজ সাইবার-আক্রমণ শুরু করবে মর্মে গত ৩১ জুলাই ২০২৩ তারিখে প্রকাশ্যে তাদের অভিপ্রায় ব্যক্ত করেছে। উক্ত সাইবার-আক্রমণ হতে মন্ত্রণালয় ও সংস্থার ডিজিটাল অবকাঠামো নিরাপদ রাখার লক্ষ্যে বাংলাদেশ কম্পিউটার কাউন্সিল এবং বিজিডিই-গভ সার্ট সতর্কতামূলক নির্দেশনা জারি করেছে (কপি সংযুক্ত)।

০২। এমতাবস্থায়, বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি) হতে প্রাপ্ত ই-মেইল এবং বিজিডি ই-গভ সার্ট-এর নির্দেশনা সংবলিত সতর্কতা জারি সংক্রান্ত পত্র এতদসংগে প্রেরণ করা হলো। তার দপ্তর/অধিশাখা/শাখা এবং সংস্থার ডিজিটাল অবকাঠামো নিরাপদ রাখার নিমিত্তে বিসিসি এবং বিজিডি ই-গভ সার্ট-এর নির্দেশনাসমূহ যথাযথভাবে প্রতিপালন করার জন্য নির্দেশক্রমে অনুরোধ করা হলো।

সংযুক্তি: বর্ণনামতে।

৮-৮-২০২৩
মোঃ মেহেদী হাসান
প্রোগ্রামার
ফোন: ০২-৫৫১০১০২৪
ফ্যাক্স: ৯৫১৫৪৯৯
ইমেইল: mehedi@mocat.gov.bd

বিতরণ :
১) সংস্থা প্রধান (সকল), বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়
২) অতিরিক্ত সচিব (সকল), বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়, ঢাকা
৩) যুগ্মসচিব (সকল), বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়, ঢাকা
৪) উপসচিব (সকল), বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়, ঢাকা
৫) সিনিয়র সহকারী সচিব (সকল), বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়, ঢাকা

স্মারক নম্বর: ৩০.০০.০০০০.০২৩.৯৯.০০২.২১.৮১/১(২)

তারিখ: ২৪ শ্রাবণ ১৪৩০
০৮ আগস্ট ২০২৩

০৮ আগস্ট ২০২৩

সদয় অবগতি ও কার্যার্থে প্রেরণ করা হল:

১) মাননীয় প্রতিমন্ত্রীর একান্ত সচিব, প্রতিমন্ত্রীর দপ্তর, বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়

২) সচিবের একান্ত সচিব, সচিবের দপ্তর, বেসামরিক বিমান পরিবহন ও পর্যটন মন্ত্রণালয়

৮-৮-২০২৩
মোঃ মেহেদী হাসান
প্রোগ্রামার

From: Data Center/BCC
To:
Cc: Rezwana Sharmin/BCC@BCC
Bcc: Mehedi/MOCAT

Date: Tuesday, August 08, 2023 10:32AM
Subject: Urgent Security Advisory Email: Potential Cyber Attack Alert - Please Exercise Caution

---

Dear Sir,
We hope this email finds you well. We are writing to inform you about **a potential cyber-attack that is expected on 15 august 2023** (Ref link: https://www.cirt.gov.bd/situational-alert-aug-2023/). As part of our commitment to your safety and security, we want to ensure that you are aware of this potential threat and take necessary precautions to safeguard your accounts and personal information.
The cybersecurity landscape is constantly evolving, and cybercriminals are becoming increasingly sophisticated in their attacks. To protect yourself and our organization from potential risks, we urge you to remain vigilant and follow these essential security guidelines:

- Ø **Avoid Clicking Suspicious Links:**
  - Be cautious when clicking on links in emails, especially from unknown senders. Hover your mouse over the link to check the destination URL before clicking.
- Ø **Exercise Caution with Email Attachments:**
  - Refrain from downloading attachments from unfamiliar sources or if you were not expecting the email. Malicious attachments can contain malware that may compromise your system.
- Ø **Verify Email Sender:**
  - Verify the sender's email address and look for any signs of suspicious activity or impersonation attempts. Cybercriminals often use email spoofing to appear legitimate.
- Ø **Be Wary of Phishing Emails:**
  - Be cautious of emails that request sensitive information, such as passwords, financial details, or personal data. Legitimate organizations will not ask for such information via email.
- Ø **Report Abnormalities:**
  - If you encounter any unusual activity, suspicious emails, or unexpected system behavior, please report it immediately to our IT support team.
- Ø **Keep Software Up-to-Date:**
  - Ensure that your devices and software are regularly updated with the latest security patches and updates.
- Ø **Use Strong and Unique Passwords:**
  - Always use strong passwords and avoid reusing passwords across different platforms.

We are actively monitoring the situation and have enhanced our security measures to protect our systems and your data. Nevertheless, your vigilance and proactive approach to cybersecurity are crucial in thwarting potential threats.
If you come across any suspicious activity, emails, or links, please immediately report them to our National Data Center support team at **email: datacenter@bcc.gov.bd or call us at +88 02 55006840.**
Your safety and security are of very importance to us, and we remain committed to providing a secure environment for all our users. Together, we can effectively combat potential cyber threats and keep our systems protected.

Thank you for your cooperation and understanding.

Regards

National Data Center Operation Team
Bangladesh Computer Council (BCC)
Phone: +88 02 55006840

From: Data Center/BCC

To:

Cc: ED BCC/BCC@BCC, Saiful Alam Khan/BCC@BCC, Hasan U Jaman/BCC@BCC, Ringko Kabiraj/BCC@BCC, Biswajit Tarapdar/BCC@BCC, Rezwana Sharmin/BCC@BCC, Md. Mamun Kabir/BCC@BCC, Al Amin/BCC@BCC, Iftekhar Ahmed/BCC@BCC, Md Saleh Ahmed/BCC@BCC, Md Iqbal Mahmood/BCC@BCC, Abdullah Al-Safy/BCC@BCC, Samin Saksiat Zaman/BCC@BCC, Shishir Kanti Nath/BCC@BCC, Faiad Iftikhar Rafee/BCC@BCC, Sumit Kumar Pramanik/BCC@BCC, Siddiqur Rahman/BCC@BCC, AMMER ASHRAF/BCC@BCC, MD. AHOSANULLAH/BCC@BCC, MD. ZENARUL ISLAM/BCC@BCC, Mohammad Moniruzzaman/BCC@BCC

Bcc: Mehedi/MOCAT

Date: Sunday, August 06, 2023 03:09PM

Subject: Important Notice: Urgent Cybersecurity Threat Alert

Dear Respected Data Center Customer,

We want to bring to your attention regarding an important matter related to the security of your digital infrastructure.

Recently, a concerning announcement was made by certain religious and ideologically motivated underground hacker groups. On July 31st, these groups publicly declared their intention to initiate a series of cyber-attacks against Bangladesh's cyberspace on August 15th.

In response to this imminent threat, the Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) has issued this alert to raise awareness among entities responsible for critical information infrastructures (CII),financial institutions, healthcare establishments, government bodies, and private organizations.The purpose of this communication is to provide you with timely information and to encourage you to take proactive steps to safeguard your IT operations and ensure business continuity. Please take note of the attached file, which outlines recommended security measures to enhance the protection of your infrastructures.

To ensure the security of your infrastructures, we kindly request that you carefully review the attached document and implement the outlined measures. Our priority is to help you mitigate risks and maintain the integrity and availability of your critical data.

Thank you for your attention to this matter.

Regards
National Data Center Operation Team
Bangladesh Computer Council (BCC)
Phone: +88 02 55006840

Attachments:

Situational-Cyber-Threat-Alert-from-BGD-e-GOV-CIRT-4.8.2023.pdf

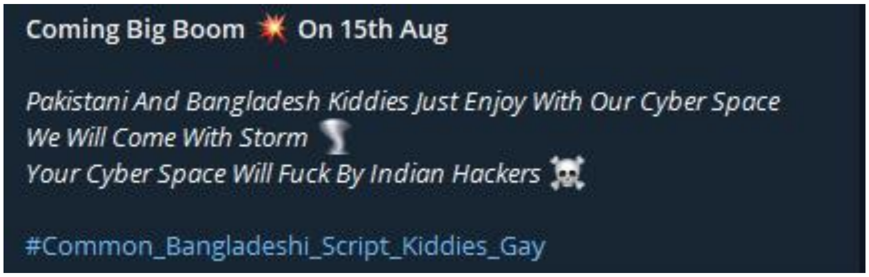
BGD e-GOV CIRT

BANGLADESH
COMPUTER
COUNCIL

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:

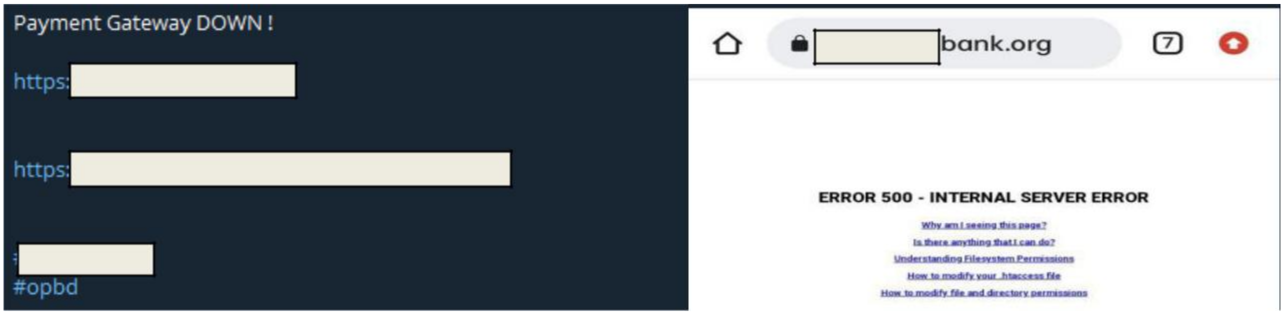
- *Distributed Denial-of-Service (DDoS) attacks*
- *Website defacements, compromising the website*
- *Using malicious PHP shells as a backdoor to drop payloads*

➢ *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]

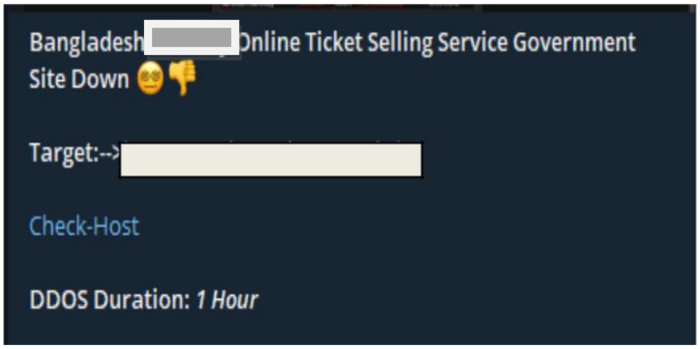
[redacted]
#opbd

[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.

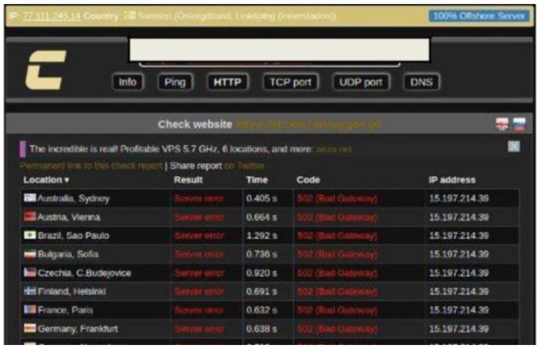


Bangladesh[redacted]Online Ticket Selling Service Government Site Down 😵👎

Target:-->[redacted]

Check-Host

DDOS Duration: *1 Hour*



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

[redacted]

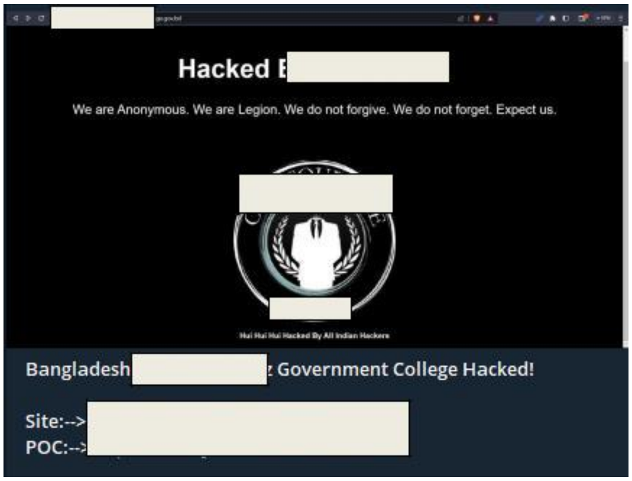
Check website [illegible]

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: [illegible]

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]

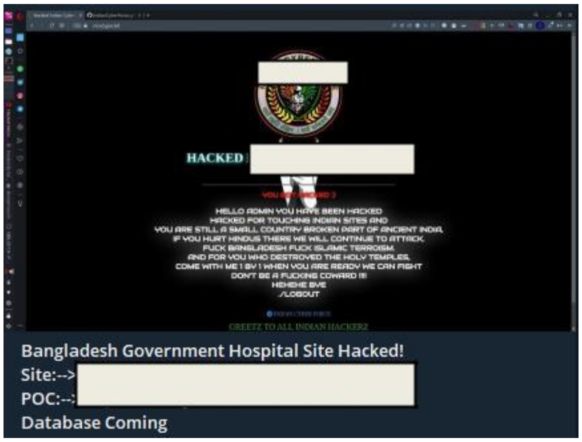
[redacted]

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 GOT HACKED :)

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

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

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