



BGD e-GOV CIRT

TLP: CLEAR



CYBER THREAT ADVISORY

**EMERGING PHISHING ATTACK ON
CYBER SPACE OF BANGLADESH**



[This page is intentionally left blank]

BGD e-GOV CIRT

TLP: CLEAR

Distribution: Public

Type of Threat: Phishing E-Mail

Date: 12 January 2025

Executive Summary

Recently, we have observed a surge in phishing attacks targeting various government organizations, law enforcement agencies, educational institutions, and others, with the attacks spreading further through compromised accounts. This campaign is targeted to steal sensitive information by impersonating official entities and leveraging malicious attachments and links. This advisory provides details on phishing email contents, Indicators of Compromise (IOCs), and detection rules to raise awareness and enhance security.

Most Targeted Sectors

- Government Organizations
- Law Enforcement Agencies
- Educational Institutions

Breakdown of Phishing Email Contents

1. Subject and Sender:

- Subject lines mimic official communication such as security notifications or updates.
- Sender addresses are spoofed to appear legitimate, often resembling government or organizational email domains.

2. Body Content:

- Formal greetings and language to establish authenticity.
- Request for urgent action, such as clicking links or downloading attachments.
- References to official-sounding documents or procedures.

3. Attachments:

- Files with extensions like .rar, .pdf, .url, .html, and renamed files like -ms to bypass filters.

4. Phishing Links:

- Redirect to fake login pages or forms that collect sensitive information.

Phishing Email Analysis

Main Suspicious Link

[https://mail-mod-gov-bd-account-data-file\[.\]netlify.app/data\[.\]html?pdf=](https://mail-mod-gov-bd-account-data-file[.]netlify.app/data[.]html?pdf=)

Domain: *mail-mod-gov-bd-account-data-file[.]netlify[.]app*

- This is a subdomain of netlify.app, commonly used for hosting free websites.
- The domain mimics a government-related name (gov-bd) to appear legitimate.

Path: */data[.]html*

The generic filename (data.html) does not align with the official communication of sensitive documents.

Query Parameter: *[?] pdf=*

No actual PDF is linked, further raising suspicion.

Alternate Download Link

[https://mail\[.\]coastguard.govmm\[.\]org/ULfwhxNc](https://mail[.]coastguard.govmm[.]org/ULfwhxNc)

Another suspicious link targeting users with a government-like domain to appear legitimate.

Generic Placeholder Links

<https://briefcase>

<https://remove>

These links are non-functional and are likely placeholders. The use of these links indicates a lack of legitimacy as no reputable sender would include such incomplete URLs.

Indicators of Phishing

Domain Spoofing: The domain name *mail-mod-gov-bd-account-data-file* is designed to mimic official government domains but is hosted under *netlify.app*, a free hosting service.

Non-functional Links: Placeholder links (*https://briefcase*, *https://remove*) highlight a lack of legitimacy.

Attachment Mismatch: The email mentions an attachment (e.g., *Letter for Security Algeria Ambassador visit to Coxsbazar.pdf*), but the link leads to a suspicious page instead of an actual file.

Content Encoding: The email content is encoded (e.g., *quoted-printable*), making it harder to analyze at a glance.

Examples of Phishing Emails

Sir,
Assalamu Alaikum.

Subject letter attached for your kind action please. Please see the attachment

Best Regards.

[Redacted]

[MAIN KEY POINTS OF CAS VISIT T... .pdf](#)

<https://mail.coastguard.govmm.org/ULfwhNc>

Letter for Security_Algeria Ambassador visit to Coxsbazar

From: [Redacted] <[Redacted]@gov.bd>
To: [Redacted] <[Redacted]@gov.bd>

Assalamualikum,

Please find the subject mentioned attachment for your information and necessary action.

With best regards

[Redacted]

New sign in attempt from China 50 min
From: [Redacted] <[Redacted]@gov.bd>
To: [Redacted] <[Redacted]@gov.bd>
January 8, 2025 12:06 PM

New sign in attempt

This sign in was on:

Device: chrome, linux
When: January 08, 2025 at 10:51:31 AM PDT
Where: China
64-155.205.00

If this was you, you're all set.

If this wasn't you:
Please take these steps to secure your account.

1. Review your phone numbers and email addresses and remove the ones that don't belong to you. [Secure your account](#)

URL: [https://mail-\[Redacted\]@gov.bd-account-error-issues.netlify.app/mail?afd=\[Redacted\]@gov.bd](https://mail-[Redacted]@gov.bd-account-error-issues.netlify.app/mail?afd=[Redacted]@gov.bd)

[Letter for Security_Algeria Ambassador visit to Coxsbazar.pdf \(2.2 MB\) Download | Briefcase | Remove](#)

URL: [https://mail-\[Redacted\]@gov-bd-account-data-file.netlify.app/data.html?pdf=\[Redacted\]@gov.bd](https://mail-[Redacted]@gov-bd-account-data-file.netlify.app/data.html?pdf=[Redacted]@gov.bd)


Letter for Norioco China updated Bridge vehicle mounted Security System in Coxsbazar full Details.

From: [Redacted] <[Redacted]@gov.bd>
To: [Redacted] <[Redacted]@gov.bd>
Subject: [Redacted]

[Letter for Norioco China updated Bridge vehicle mounted Security System in Coxsbazar full Details.pdf \(2.2 MB\) Download | Briefcase | Remove](#)

Assalamualikum,

Please find the subject mentioned attachment for your information and necessary action.
With best regards


Phone: [Redacted]
Web: [Redacted]
Email: [Redacted]

Registration Pending of Cloud Service Platform 14 min
From: [Redacted] <[Redacted]@gov.bd>
To: [Redacted] <[Redacted]@gov.bd>
December 28, 2024 10:19 PM

Dear Sir,

We are pleased to inform you that we are registering our cloud service platform to new Secure service platform to enhance your email experience.

Registration Details:

- Start: 28 December, 2024 Saturday 09:00 pm to Jan 2, 2025 Thursday 09:00 am (Local Time)
- Activity: Cloud Service Platform Registration

During this transition, there may be a temporary interruption in email services as the changes propagate. While we aim for a smooth process, please plan accordingly.

Action Required:

Registration Link: [https://\[Redacted\]@gov.bd](https://[Redacted]@gov.bd)

Thank you for your understanding and cooperation as we work to provide you with a better email experience.

Regards
[Redacted]

BGD e-GOV CERT

Norico Bridge Details.
From: [redacted] <[redacted]@gov.bd>
To: [redacted] <[redacted]@mil.bd>

Assalamualikum,

Please find the subject mentioned attachment for your information and necessary action.
With best regards

[redacted]
[redacted]

[Norico Bridge Details \(2.2 MB\)](#) Download | Briefcase | Remove
URL: <https://tinyurl.com/3ttj6xaj>

From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted] <[redacted]@gov.bd>

Assalamualikum,

Please find the subject mentioned attachment for your information and necessary action.
With best regards

[redacted]
Deputy Director
Directorate of Project

[Letter for Security, Algeria Ambassador visit to Cox's Bazar](#)
URL: <https://mail.gov.bd/account-data-file/netlify.app/data.html/pdf>

Follow-up on Outstanding Invoice

1 message

From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]

December 17, 2024 5:53 PM

[redacted]

Show more...

Please find the link below for the pending Invoice No. 228-365484

[https://\[redacted\]gov.bd/#/acs/invoice/Updated?IN=228365484](https://[redacted]gov.bd/#/acs/invoice/Updated?IN=228365484)

URL: <https://finance-gov-bd.b-cdn.net/>

Reply - Reply to All - Forward - More Actions

Incident Report in Control Room
From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]
December 27, 2024 12:33 PM

[Report-Controlroomurl \(51 B\)](#) Download | Briefcase | Remove

Dear Team,

There has been a severe incidence occurred inside the control room of Paharika Express. The details of the incident, including the circumstances and other relevant information, have been documented in the attached report. Please review the attached document for all the specifics.

Regards
Control Room Dhaka

Security Measures Following Proclamation Announcement
From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]
December 31, 2024 11:59 AM

Dear Sir,

After the announcement of the Proclamation of the July Uprising and the subsequent riots at Agratala Station., Please prioritize increased security at all railway stations to ensure uninterrupted service. [Proclamation_of_the_July_Security_Guidelines.pdf](#)

Best regards, URL: https://gov-bd.b-cdn.net/Proclamation_of_the_July_Uprising.html

Operations Manager

BAESA Meeting Points 24-Dec
From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]
December 24, 2024 5:19 PM

[BAESA-24rar \(10.6 KB\)](#) Download | Briefcase | Remove

Please Find the attached Document

Urgent Incident at Kamlapur Station Tracks
From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]
January 6, 2025 1:34 PM

[BH-6597_reports.pdf.searchConnector-ms \(265 B\)](#) Download | Briefcase | Remove

Dear Sir,

A serious incident has occurred on the tracks of Kamlapur Station. Kindly find the attached PDF containing detailed information and recommended actions. Your prompt attention to this matter would be greatly appreciated.

Notification of Network Disruption and Potential Power Cut

1 message

From: [redacted] <[redacted]@gov.bd>
Bcc: [redacted]

January 6, 2025 5:42 PM

Show more...

[Disruption-report-sheet.searchConnector-ms \(265 B\)](#) Download | Briefcase | Remove

Dear Sir,

We would like to inform you that there has been a network disruption in the line affecting certain areas of your facility. As a result, there is a possibility of a slight power cut in the affected zones.

Please find the attached document for a detailed list of the disturbed facilities and the timings of the potential disruptions. We are actively working to resolve the issue, and we will provide you with updates as necessary.

Indicators of Compromise (IOCs):

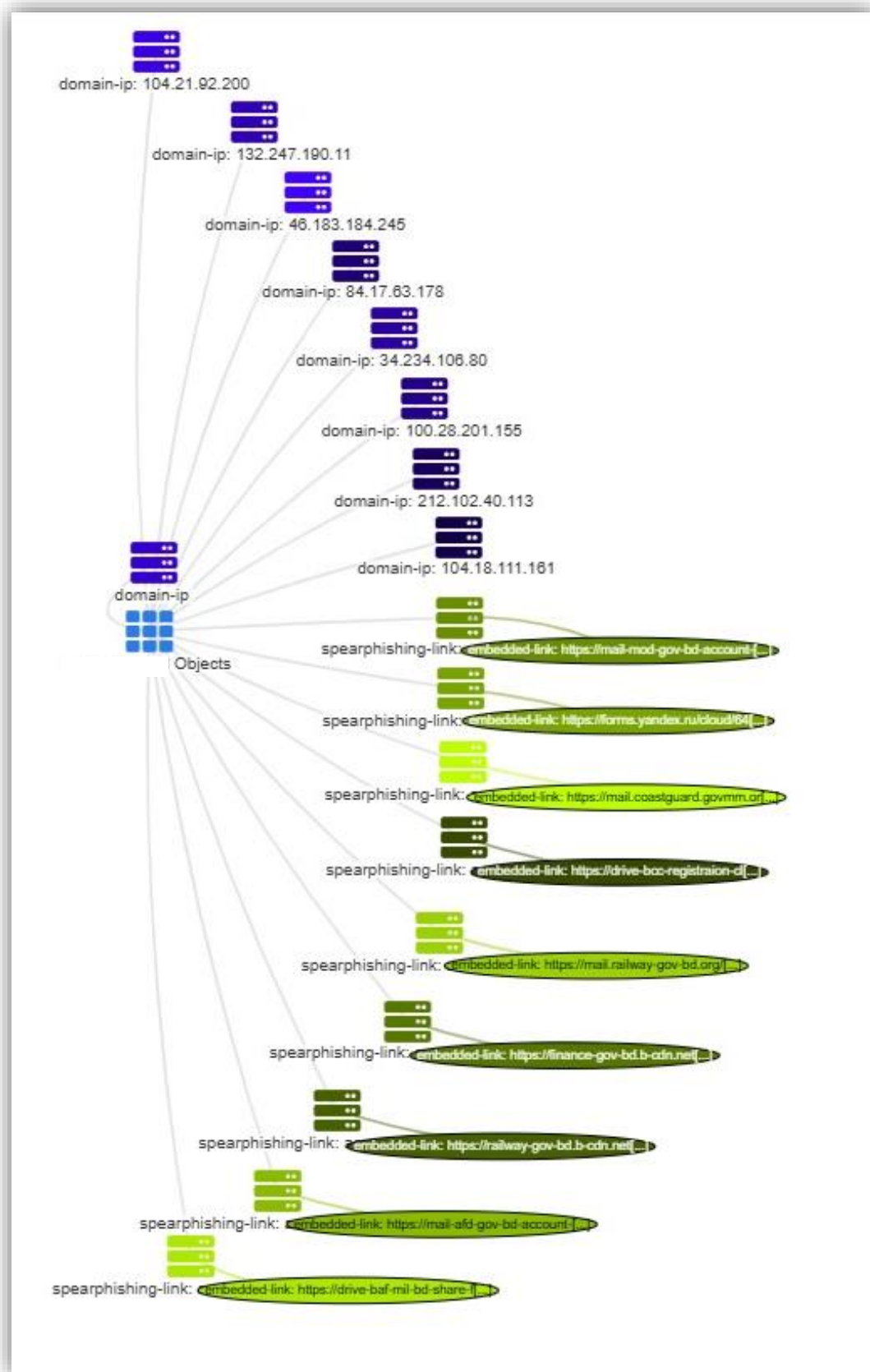
IP Addresses	34.234.106[.]80
	104.21.92[.]200
	84.17.63[.]178
	212.102.40[.]113
	100.28.201[.]155
	132.247.190[.]11
	104.18.111[.]161
	46.183.184[.]245
Attached File Extension	.rar
	.pdf
	.url
	.html
	-ms (file renamed as -ms to bypass filters)
Phishing Links	https[:]//drive-baf-mil-bd-share-file.netlify.app/airforce%20drive%20share
	https[:]//drive-bcc-registraion-cloud-storage.netlify.app/bcc%20drive%20share
	https[:]//railway-gov-bd.b-cdn.net/Proclamation%20of%20the%20July%20Uprising.html
	https[:]//railway-gov-bd.b-cdn.net/Proclamation%20of%20the%20July%20Uprising.html
	https[:]//mail-mod-gov-bd-account-data-file.netlify.app/data.html?pdf=
	https[:]//forms.yandex.ru/cloud/64d311e643f74f24f282c9e6
	https[:]// mail-afd-gov-bd-account-error-issues.netlify.app/afd.html?afd=admin_dte@afd[.]gov.bd
	https[:]//mail.railway-gov-bd.org
https[:]//mail.coastguard.govmm.org/ULfwhxNc	

MITRE ATT&CK Mapping:

Tactic: Initial Access ([TA0001](#))

- **Technique:** Spear Phishing Link ([T1566.002](#))
- **Technique:** Spear Phishing Attachment ([T1566.001](#))

Overview of Phishing Campaign Infrastructure IP addresses and links:



Technical Detection Rules: (BGD e-GOV CIRT)

Note:

The following rules are provided as **samples** to assist technical teams in utilizing Indicators of Compromise (IoCs) for **threat hunting** or **threat detection** purposes. These rules may need to be **customized** to align with the specific fields and configurations of your **SIEM** and other security monitoring tools. Always review and adapt these rules to fit your operational environment and security requirements.

Suricata Rules

```
alert http any any -> any any (msg:"Phishing URL detected - mail-  
mod-gov-bd"; content:"mail-mod-gov-bd-account-data-file"; http_host;  
classtype:trojan-activity; sid:1000001; rev:2;)  
  
alert http any any -> any any (msg:"Phishing URL detected - Coast  
Guard"; content:"mail.coastguard.govmm.org"; http_host;  
classtype:trojan-activity; sid:1000002; rev:2;)  
  
alert ip any any -> any any (msg:"Phishing IP detected -  
46.183.184.245"; ip_dst:46.183.184.245; classtype:trojan-activity;  
sid:1000003; rev:2;)  
  
alert ip any any -> any any (msg:"Phishing IP detected -  
34.234.106.80"; ip_dst:34.234.106.80; classtype:trojan-activity;  
sid:1000004; rev:2;)
```

Sigma Rules

- **Sigma Rule 1: Suspicious IP Address Connection**

```
title: Suspicious IP Address Connection
description: Detects connections to known malicious IP addresses.
author: CTI unit of BGD e-GOV CIRT
logsource:
  category: network
  product: network
detection:
  selection:
    # Replace 'network.src_ip' and 'network.dest_ip' with the
    # appropriate fields for your platform
    # Example field mappings:
    # - Splunk: src_ip, dest_ip
    # - Elastic ECS: source.ip, destination.ip
    # - Wazuh: data.srcip, data.dstip
    network.src_ip|endswith:
      - '34.234.106.80'
      - '104.21.92.200'
      - '84.17.63.178'
      - '212.102.40.113'
      - '100.28.201.155'
      - '132.247.190.11'
      - '104.18.111.161'
      - '46.183.184.245'
    network.dest_ip|endswith:
      - '34.234.106.80'
      - '104.21.92.200'
      - '84.17.63.178'
      - '212.102.40.113'
      - '100.28.201.155'
      - '132.247.190.11'
      - '104.18.111.161'
      - '46.183.184.245'
  condition: selection
fields:
  - src_ip
  - dest_ip

# Guidelines for Adapting This Rule:
# 1. Understand your platform's field names:
#   - Splunk: src_ip, dest_ip
#   - Elastic ECS: source.ip, destination.ip
#   - Wazuh: data.srcip, data.dstip
# 2. Identify relevant fields in your logs by inspecting sample
#    events.
# 3. Replace the field names in 'detection' with your platform-
#    specific field names.
# 4. Use tools like Uncoder.io for automated translations and manual
#    adjustments as needed.
# 5. Test the translated query on your platform to validate results.
```

- **Sigma Rule 2: Phishing Link Detected**

```
title: Phishing Link Detected
description: Detects access to known phishing links.
author: CTI unit of BGD e-GOV CIRT
logsource:
  category: network
  product: network
detection:
  selection:
    # Replace 'network.http_uri' with the appropriate fields for
    your platform
    # Example field mappings:
    # - Splunk: uri
    # - Elastic ECS: url.path
    # - Wazuh: http.url
    network.http_uri|endswith:
      - 'drive-baf-mil-bd-share-file.netlify.app'
      - 'drive-bcc-registraion-cloud-storage.netlify.app'
      - 'railway-gov-bd.b-cdn.net'
      - 'finance-gov-bd.b-cdn.net'
      - 'mail-mod-gov-bd-account-data-file.netlify.app'
      - 'forms.yandex.ru'
      - 'mail-afd-gov-bd-account-error-issues.netlify.app'
      - 'mail.railway-gov-bd.org'
      - 'mail.coastguard.govmm.org'
    network.http_uri|contains:
      - 'drive-baf-mil-bd-share-file.netlify.app'
      - 'drive-bcc-registraion-cloud-storage.netlify.app'
      - 'railway-gov-bd.b-cdn.net'
      - 'finance-gov-bd.b-cdn.net'
      - 'mail-mod-gov-bd-account-data-file.netlify.app'
      - 'forms.yandex.ru'
      - 'mail-afd-gov-bd-account-error-issues.netlify.app'
      - 'mail.railway-gov-bd.org'
      - 'mail.coastguard.govmm.org'
  condition: selection
fields:
  - http_uri

# Guidelines for Adapting This Rule:
# 1. Understand your platform's field names:
#   - Splunk: uri
#   - Elastic ECS: url.path
#   - Wazuh: http.url
# 2. Identify relevant fields in your logs by inspecting sample
    events.
# 3. Replace the field names in 'detection' with your platform-
    specific field names.
# 4. Use tools like Uncoder.io for automated translations and manual
    adjustments as needed.
# 5. Test the translated query on your platform to validate results.
```

Actions Required:

To mitigate the risk, the following measures are recommending:

1. Be Alert:

- Avoid clicking on unknown links or downloading suspicious attachments.
- Verify sender email addresses carefully to detect impersonation.

2. Report Suspicious Emails:

- Forward phishing emails to the IT/security team or use “Report Phishing” tools.

3. Protect Credentials:

- Never share login details via email or on unofficial websites.
- Enable multi-factor authentication (MFA) for all critical accounts.

4. Training and Awareness:

- Participate in phishing awareness sessions and simulated tests.
- Stay updated on common phishing tactics and red flags.

5. IOC Monitoring:

- Use the provided Indicators of Compromise (IOCs) list, Suricata Rule (for Network Traffic) and Sigma Rules (for SIEM Query) to create threat hunt and detection rules.
- Continuously monitor systems and logs for suspicious activity.

6. System Security:

- Patch and update all systems and software to prevent vulnerabilities.
- Apply the principle of least privilege to user accounts and audit permissions regularly.
- Use email filtering and sandboxing to block malicious attachments or links.

7. Incident Response:

- Ensure an active and tested incident response plan is in place.
- Act promptly on reported phishing incidents to contain threats.
- Report or inform BGD e-GOV CIRT, BCC regarding any IOC's or suspicious activities within your infrastructure, through mail id: cirt@cirt.gov.bd or cti@cirt.gov.bd