Incident Response Report

Incident Title: Suspicious Academic Offer via Email
Date of Report: 24 August 2025
Reported By: Hrushikesh
Incident Date: 19 August 2025
Source Email: maheshimp@proton.me
Recipient Email: training@asdacademy.in
Subject Line: Urgent Bumper Offer – Upload the Test

Summary of Incident

An unsolicited email was received by ASD Academy from an external sender, Mahesh Rai, offering students a chance to improve their grades by uploading assignments via a linked HTML file. The email was titled as an "Urgent Bumper Offer" and included an attachment named hi.html. The message encouraged students to download the file and submit their assignments through a portal, claiming it would boost their exam scores.

Artifacts Collected

- **Email File:** Urgent Bumper Offer
- **Attachment:** hi.html
- **Sender Domain:** proton.me
- **Source Email:** maheshimp@proton.me

Initial Analysis

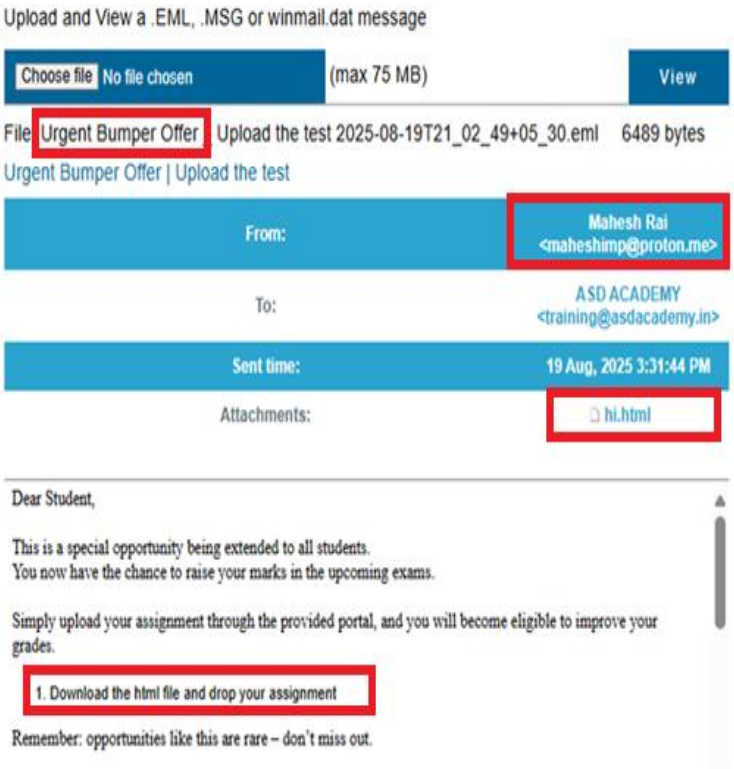
- The email uses urgency and academic incentives to lure recipients.
- The HTML attachment could redirect to a malicious site or collect sensitive data.
- No official institutional branding or verification is present.
- The sender is not affiliated with ASD Academy.

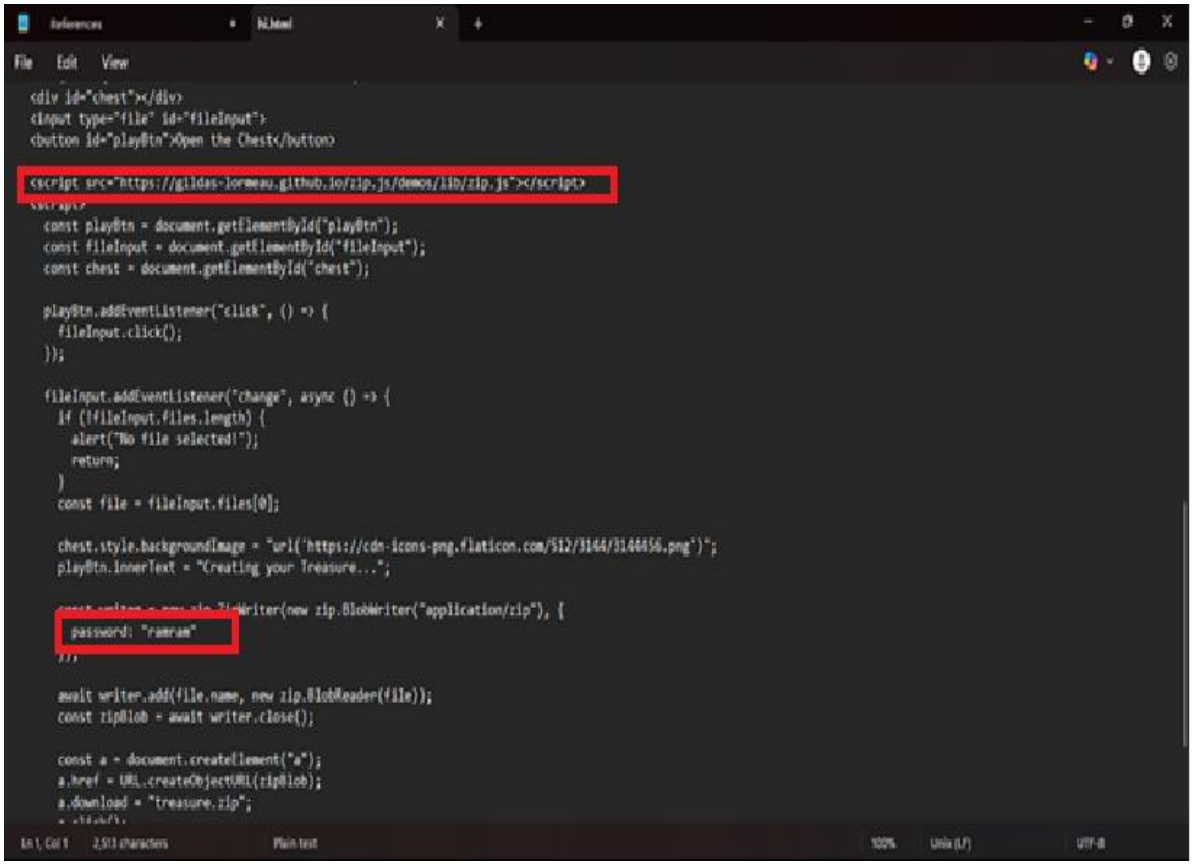
Technical Analysis of hi.html

- The selected file is zipped using zip.js and downloaded as treasure.zip
- A hardcoded password "ramram" is used to encrypt the ZIP file

Recommended Actions

1. **Do Not Interact** with the HTML file or any links it may contain.
2. **Quarantine the Email** and attachment for further forensic analysis.
3. **Notify Students** about the suspicious message and advise caution.
4. **Block Sender Domain** (proton.me) if deemed necessary.
5. **Conduct a Security Scan** on any systems that may have accessed the file.
6. **Report to Authorities** if phishing or fraud is confirmed.




File Edit View

<input type="file" id="fileInput">
<button id="playBtn">Open the Chest</button>
<script src="https://gildas-lormeau.github.io/zip.js/demos/lib/zip.js"></script>
const playBtn = document.getElementById("playBtn");
const fileInput = document.getElementById("fileInput");
const chest = document.getElementById("chest");
playBtn.addEventListener("click", () => {
fileInput.click();
});
fileInput.addEventListener("change", async () => {
if (!fileInput.files.length) {
alert("No file selected!");
return;
}
const file = fileInput.files[0];
chest.style.backgroundImage = "url('https://cdn-icons-png.flaticon.com/512/3144/3144656.png')";
playBtn.innerText = "Creating your Treasure...";
password: "rameram"
await writer.add(file.name, new zip.BlobReader(file));
const zipBlob = await writer.close();
const a = document.createElement("a");
a.href = URL.createObjectURL(zipBlob);
a.download = "treasure.zip";
Ln 1, Col 1
2,513 characters
Plain text
100%
Unix (LF)
UTF-8