

Phishing Incident Report-Credential-Capturing Email Analysis

Phishing Incident Report-Credential-Capturing Email Analysis

1. General Information:

Attribute	Details
Date:	01/08/2023, 21:22:47
Subject:	Microsoft account unusual signin activity
To:	phishing@pot
From:	Microsoft account team
Reply-To:	N/A
Return-Path:	N/A
Sender IP:	103[.]225[.]77[.]255
Resolve Host:	The IP address is from a server in Russia, which could be suspicious.
Message-ID:	Not provided in the Email body

2. URLs

Status	Comments	URL
Malicious (Phishing)	Confirmed – The URL is not a legitimate Microsoft domain. It is hosted on "vercel.app," a platform for app deployment, not affiliated with Microsoft. This strongly indicates phishing.	hxxps[:]//]mc4-two[.]vercel[.]app/

3. Attachment

Attachment Name	MD5	SHA1	SHA256	Description
N/A	N/A	N/A	N/A	No - Attachment in this email.

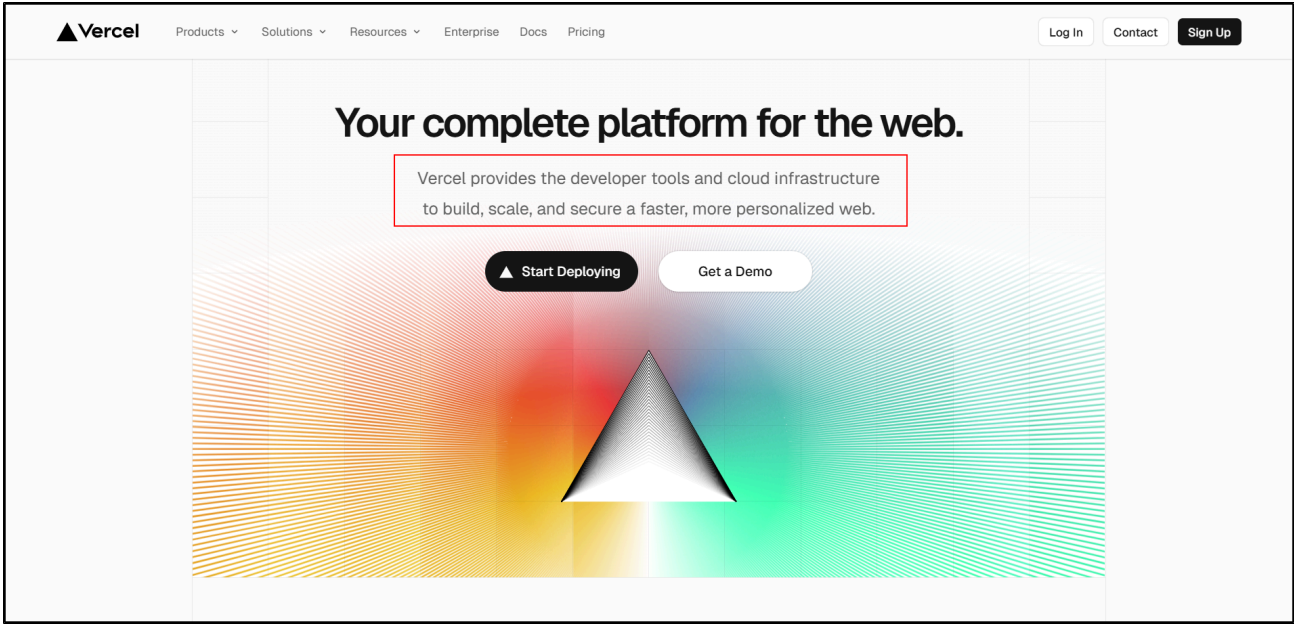
4. Artifact Analysis

4.1 Sender Analysis:

- The email appears to be from the "Microsoft account team" However, the unusual recipient (**phishing@pot**) suggests a phishing attempt.

4.2 URL Analysis:

- **URL:** hxxps[:]//]mc4-two[.]vercel[.]app/
- **Type:** Malicious (Phishing).
- **Comments:** The URL is hosted on the "Vercel platform," which is commonly used for deploying web apps. This platform is not associated with Microsoft, and using it in a phishing email is a red flag. Hence, the email is part of a phishing attempt intended to trick users into clicking the link and entering their login details or other personal information.
- **Supporting Evidence:**



The top screenshot displays the Pulsedive Community interface for the URL `mc4-two.vercel.app`. The interface shows a sidebar with navigation options like Overview, Screenshot, Attributes, Threats, Feeds, and Comments. The main content area highlights the URL's 'Unknown risk' status and provides a list of properties including DNS, HTTP, and SSL. A 'Vercel Technologies' tag is also visible. The bottom screenshot shows a detailed analysis of the URL `https://mc4-two.vercel.app/`. It features a 'Community Score' of 16/96, a 'Malicious' status, and a list of categories including 'Phishing' and 'Fraud'. The analysis also includes a 'History' section with submission and analysis dates, and an 'HTTP Response' section showing the final URL and serving IP address.

4.3 Attachment

- No attachments were included.

5. Verdict

The email is confirmed as **malicious (phishing)**. The suspicious recipient address (**phishing@pot**) and the non-Microsoft URL indicate a phishing attempt, where the sender aims to trick users into clicking the link and stealing their personal information.

6. Defense Action

- **Do not click** on the URL.
- **Mark the Email as Phishing.**
- **Block the Sender.**
- **Delete the email immediately.**