

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.

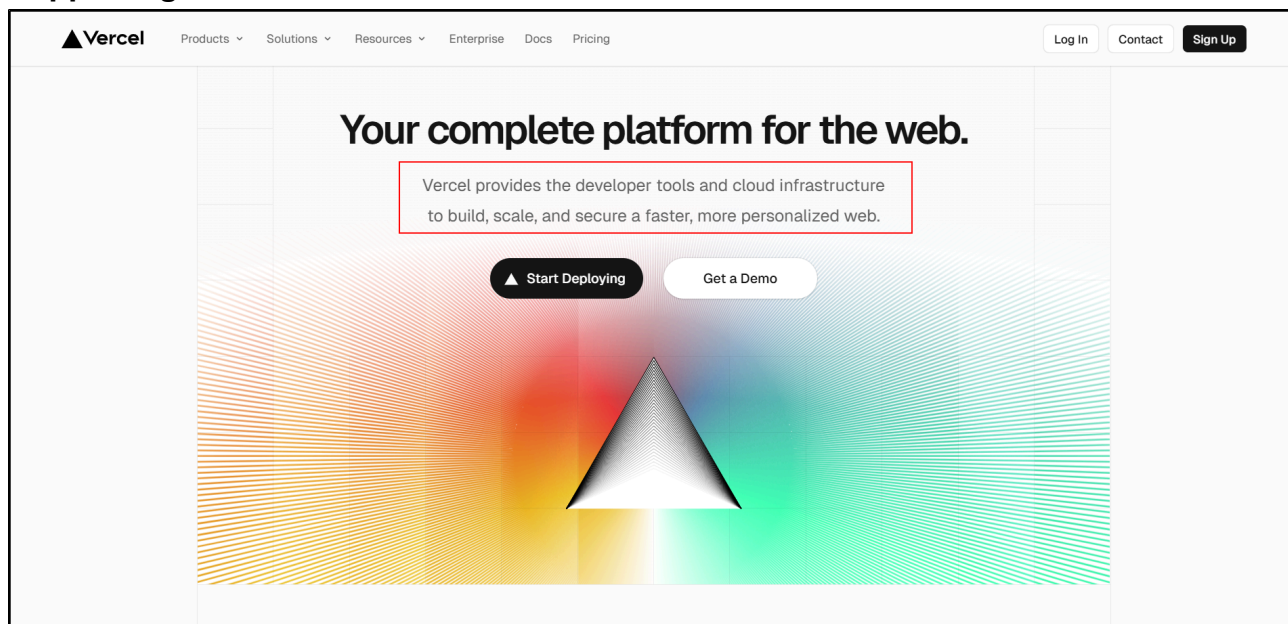
4. Artifact Analysis

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:**



mc4-two.vercel.app

Unknown risk

Integrations

- VirusTotal: Available in Pro
- Shodan: Available in Pro
- AbusIPDB: Available in Pro

Actions

- Copy Summary
- Seen
- Rescan
- Export
- Share

Highlights

- 200 HTTP status
- Subdomain
- text/html Content-type
- SSL certificate found: *.vercel.app and 1 more
- Vercel Technologies

Events

- Added: 2024-05-13 08:06:36 (7 months ago)
- Cert. issued: 2024-08-14 04:14:55 (4 months ago)
- Scanned: 2024-08-28 21:50:04 (3 months ago)
- Updated: 2024-10-08 00:43:08 (2 months ago)
- Seen: 2024-10-08 00:43:08 (2 months ago)
- Cert. expires: 2024-11-12 03:14:54 (1 month ago)

https://mc4-two.vercel.app/

16/96 security vendors flagged this URL as malicious

Community Score: -90

Status: 451

Content type: text/html, charset=utf-8

Last Analysis Date: 25 days ago

DETECTION

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Categories

- alphaMountain.ai: Malicious, Phishing (alphaMountain.ai)
- Sophos: phishing and fraud
- Webroot: Phishing and Other Frauds
- Forcepoint ThreatSeeker: malicious web sites

History

- First Submission: 2024-05-10 16:42:42 UTC
- Last Submission: 2024-11-15 05:11:07 UTC
- Last Analysis: 2024-11-15 05:11:07 UTC

HTTP Response

Final URL: https://mc4-two.vercel.app/

Serving IP Address: 76.76.21.123

Status Code

4.3 Attachment

- No attachments 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.**