Findings

Time: 2025-03-19 15:03:51 EDT
Host: N/A (Email-based activity)
IOC Domain: partners-uber[.]com
IOC IP: Unknown (email headers not provided)
Possible Malware Family: N/A (No payload observed)
Filename: N/A
SHA256 Hash: N/A

Investigation

On **2025-03-19** at approximately **15:03:51 EDT**, an email claiming to represent Uber partnerships was received from **manager@partners-uber[.]com** using the display name *"Vanessa."* The message was generic and lacked verifiable details, links, or attachments.

Analysis identified **partners-uber[.]com** as a lookalike domain impersonating Uber. WHOIS data showed the domain was recently registered **(2025-03-05)** and exhibited significant infrastructure instability, including multiple IP address and hosting provider changes, and was placed on **clientHold**, indicating registrar-level suspension.

Despite the absence of a payload, these indicators are consistent with pretexting-style phishing, where initial contact is used to establish trust prior to follow-on malicious activity. Based on this evidence, the email was classified as a confirmed **phishing attempt via brand impersonation.**

WHO / WHAT / WHEN / WHERE / WHY / HOW

WHO: Unknown sender impersonating Uber using partners-uber[.]com
WHAT: Phishing email posing as a business partnership inquiry
WHEN: 2025-03-19 15:03:51 EDT
WHERE: Email delivery; no endpoint interaction observed
WHY: Establish trust for follow-on malicious activity (pretexting/BEC-style phishing)
HOW: Lookalike domain + generic outreach from role-based sender

Analyst Next Steps

1. Block **partners-uber[.]com** at the email security gateway
2. Perform an email trace and scoping to identify additional recipients or replies.
3. Add domain and sender address to internal IOC tracking
4. Monitor for follow-up emails using Uber-themed lookalike domains

Recommendations

1. Block partners-uber[.]com at the email gateway
2. Monitor for follow-up emails using Uber-themed lookalike domains
3. Notify users and reinforce awareness of partnership-based phishing lures