PHISHING EMAIL & MALICIOUS URL INVESTIGATION REPORT

Prepared For: NexShield

Prepared By: TIJANI AYANTAYO

Date: February 19, 2026

1. EXECUTIVE SUMMARY.

As requested by NexShield, a security investigation was conducted into a suspected phishing email targeting administrative personnel. The purpose of this assessment was to analyze the email content, examine the embedded URL, determine the threat level, evaluate associated risks, and recommend mitigation strategies to prevent future attacks.

Our investigation identified multiple phishing indicators within the email, including urgent messaging, suspicious hyperlinks, and requests for credential verification. Analysis of the embedded URL revealed characteristics consistent with credential harvesting and phishing infrastructure. Based on these findings, this incident is classified as a Medium–High risk threat due to the potential compromise of administrative accounts and unauthorized access to internal systems.

—

2. SCOPE OF INVESTIGATION

The following activities were performed:

- Email Content Analysis
- URL Reputation Analysis (VirusTotal, URLscan.io, Cisco Talos)
- Domain Investigation (WHOIS Lookup)
- Risk Assessment
- Mitigation Recommendations

3. EMAIL CONTENT ANALYSIS

Key Phishing Indicators Identified:

• Urgent tone requiring immediate verification

The message pressures users to act quickly, reducing their ability to verify legitimacy.

• Deadline threatening account suspension

Creates fear to manipulate recipients into clicking the link.

• Generic sender identity (“IT Security Team”)

Legitimate internal emails usually include specific names or departments.

• Suspicious link formatting

The embedded URL appears abnormal and unrelated to the organization’s official domain.

• Credential verification request

Requests for usernames or passwords via email are strong indicators of credential harvesting.

• Possible grammar/spelling inconsistencies

Common in phishing emails and reduce authenticity

4. URL REPUTATION ANALYSIS

Corrected URL Format:

“ https://securesupport.vercel.app/ “

Tools Used:

• VirusTotal

• URLscan.io

• Cisco Talos Intelligence

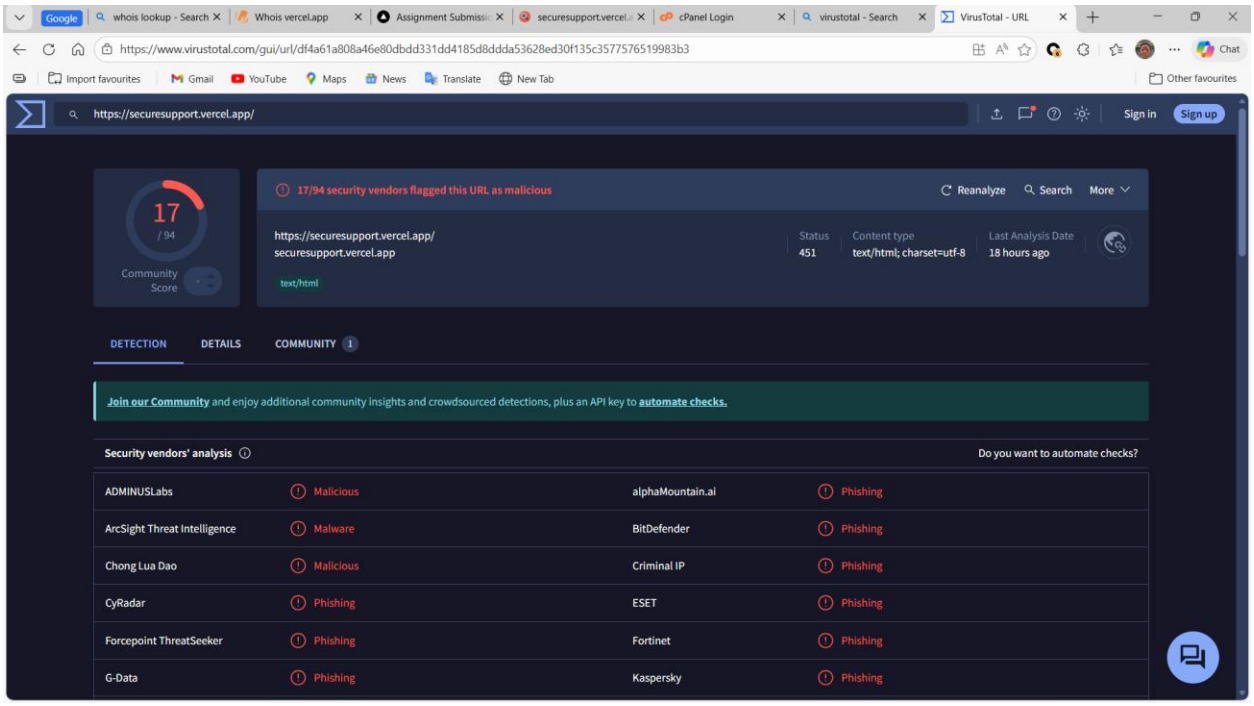
VirusTotal Findings

• Several engines flagged the URL as suspicious/phishing

• Low reputation score

• Associated with credential harvesting behavior

• Recently observed domain



Screenshot From Virustotal

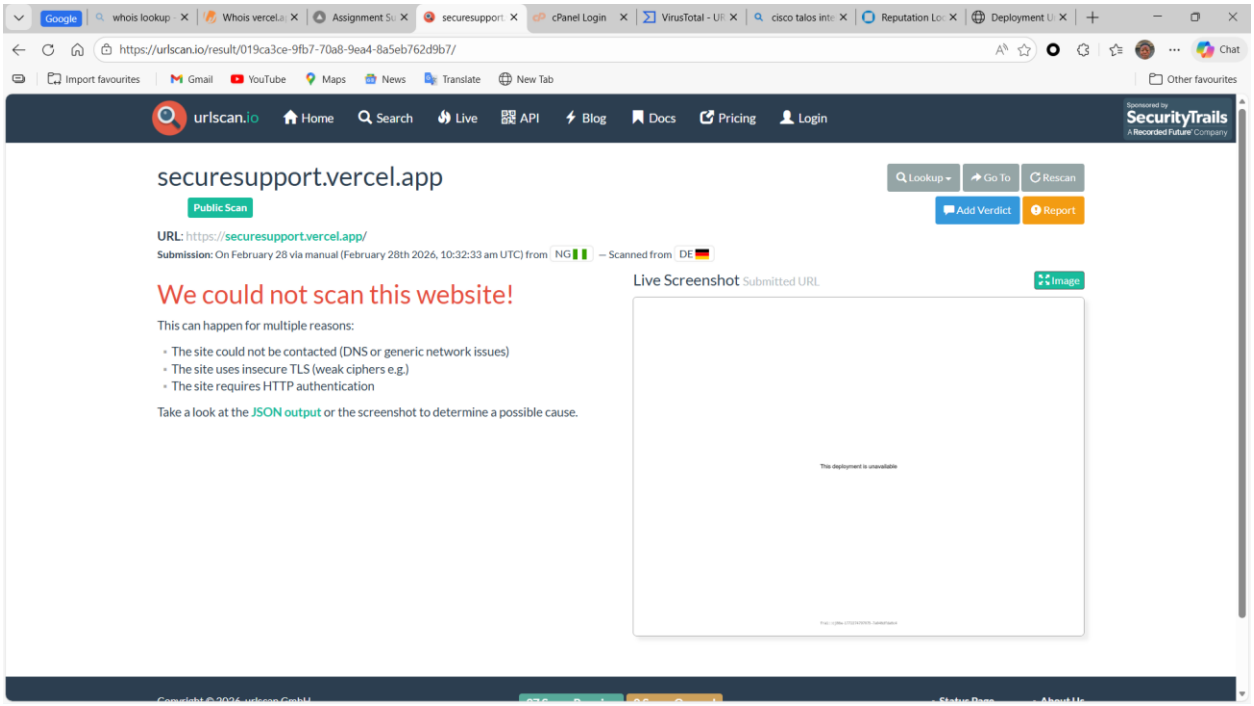
URLscan.io Findings

• Redirects to a fake login page

• Contains suspicious scripts

• Page designed to capture credentials

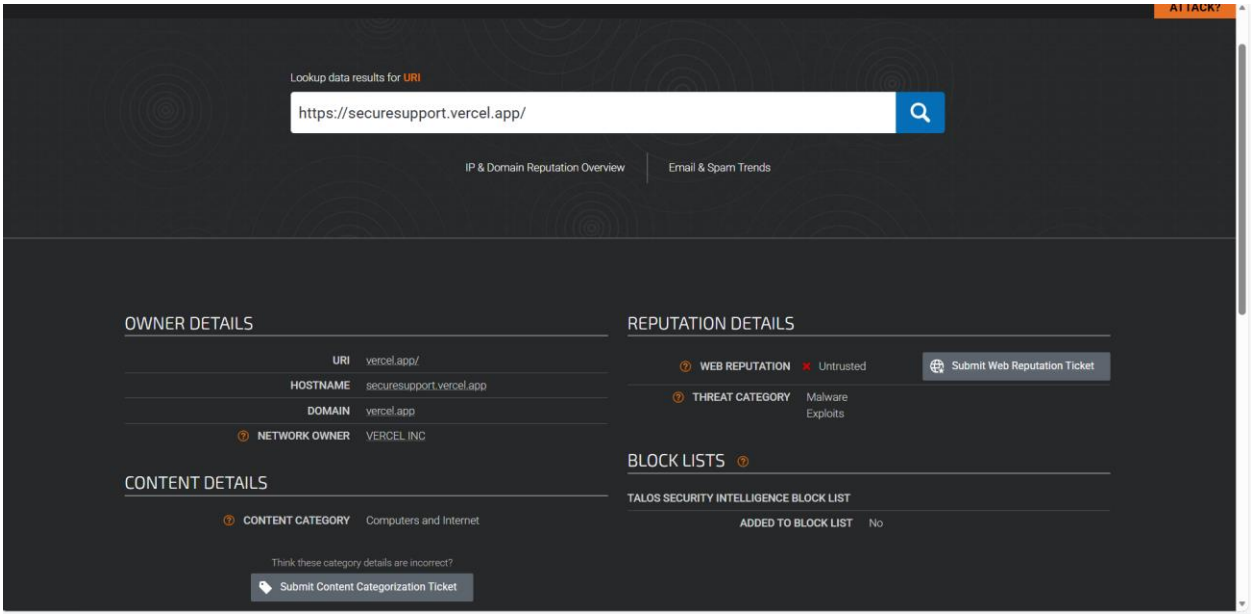
• No legitimate business content



Screenshot from urlscan.io

Cisco Talos Findings

- Poor domain reputation
- No established trust history
- Cloud-hosted infrastructure commonly abused by attackers



Screenshot from cisco talos intelligence

5. DOMAIN INVESTIGATION (WHOIS)

Base Domain:

vercel.app

Registration Details

• Registrar: Vercel Inc.

• Creation date: 2020-01-28

• Expiration date: 2036-01-28 (2020 - 2036)

• Name servers:
ns1.vercel-dns-3.com
ns2.vercel-dns-3.com
ns3.vercel-dns-3.com
ns4.vercel-dns-3.com)

• Registrant: Tucows Domains Inc

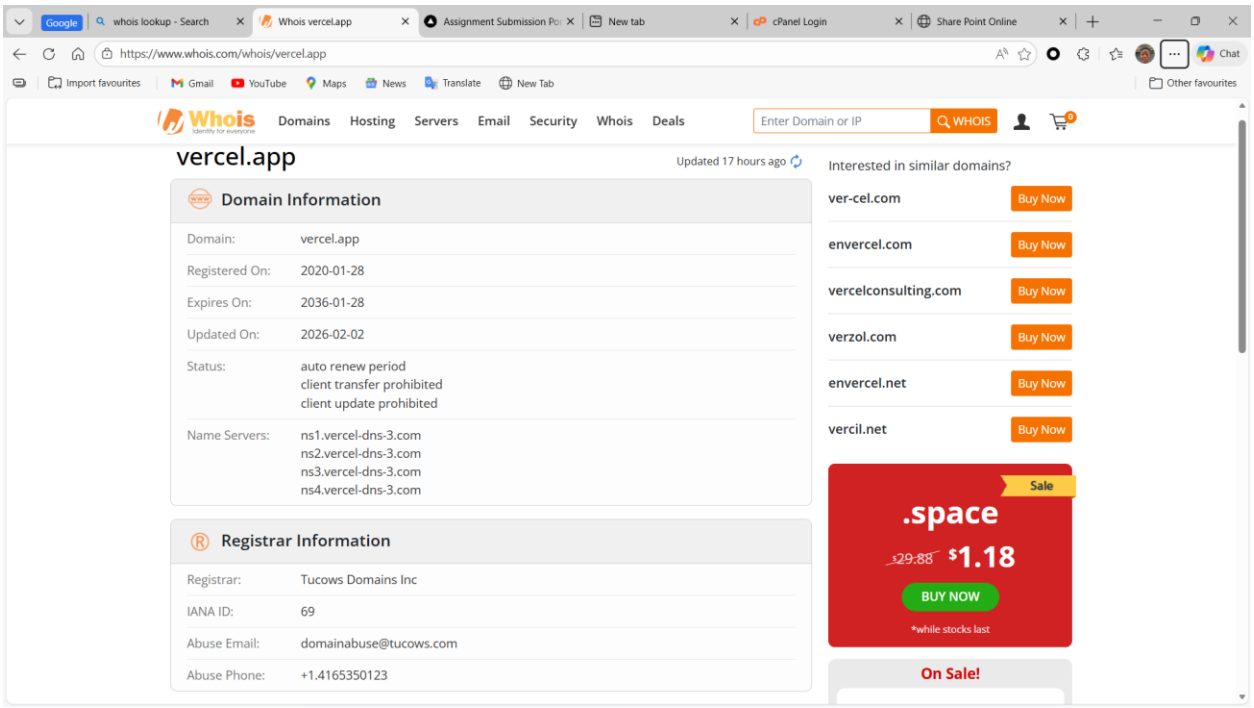
Suspicious Characteristics

• Newly created domain

• Minimal registration details

• Frequently abused cloud hosting service

These characteristics increase the likelihood that the domain is being used for phishing or temporary malicious activity.



SCREENSHOT FROM WHOIS LOOKUP

6. RISK ASSESMENT

If an employee submits credentials through the malicious link, potential consequences include:

• Administrative account compromise

• Unauthorized system access

• Lateral movement within the network

• Data exfiltration

- Malware infection
- Reputational damage
- Financial losses
- Operational downtime

Overall Risk Level: Medium–High

7. RECOMMENDATIONS

Immediate Actions

- Block malicious URL at firewall/DNS level
- Reset potentially compromised credentials
- Enforce Multi-Factor Authentication (MFA)
- Review authentication logs for suspicious activity
- Notify affected users

Long-Term Preventive Measures

- Conduct regular phishing awareness training
- Implement secure email gateway filtering
- Deploy DNS filtering and endpoint detection tools
- Enable IDS/IPS monitoring
- Strengthen password policies
- Perform regular security audits
- Enhance SIEM monitoring and alert tuning