

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

The screenshot shows the VirusTotal interface for the URL <https://secureresupport.vercel.app/>. The main summary indicates 17/94 security vendors flagged the URL as malicious. Below this, detailed information includes the URL, status (451), content type (text/html; charset=utf-8), and last analysis date (18 hours ago). The 'Community Score' is shown as 17/94. The 'DETECTION' tab is selected, showing a table of vendor analysis results:

Security vendor	Result	Do you want to automate checks?
ADMINUSLabs	Malicious	Phishing
ArcSight Threat Intelligence	Malware	Phishing
Chong Lua Dao	Malicious	Phishing
CyRadar	Phishing	Phishing
Forcepoint ThreatSeeker	Phishing	Phishing
G-Data	Phishing	Phishing
alphaMountain.ai		
BitDefender		
Criminal IP		
ESET		
Fortinet		
Kaspersky		

Screenshot From Virustotal

URLscan.io Findings

- Redirects to a fake login page
- Contains suspicious scripts
- Page designed to capture credentials
- No legitimate business content

The screenshot shows a browser window with multiple tabs open, including Google, whois lookup, Whois vercel, Assignment 5, securesupport, cPanel Login, VirusTotal, Cisco Talos, Reputation, Deployment, and others. The main content area is from urlscan.io, displaying the URL <https://urlscan.io/result/019ca3ce-9fb7-70a8-9ea4-8a5eb762d9b7/>. A banner at the top says "Sponsored by SecurityTrails A Recorded Future Company". Below it, there's a search bar with "Public Scan" selected, and buttons for "Lookup", "Go To", "Rescan", "Add Verdict", and "Report". The URL is listed as "URL: <https://securesupport.vercel.app/>". The submission information shows "Submission: On February 28 via manual (February 28th 2026, 10:32:33 am UTC) from NG 🇩🇪 — Scanned from DE 🇩🇪". A large red error message "We could not scan this website!" is prominently displayed. Below it, a list of reasons includes: "The site could not be contacted (DNS or generic network issues)", "The site uses insecure TLS (weak ciphers e.g.)", and "The site requires HTTP authentication". A note says "Take a look at the [JSON output](#) or the screenshot to determine a possible cause." A "Live Screenshot" section shows a blank white box with the text "This deployment is unavailable". At the bottom, there's a footer with links to "Status Page", "About Us", and "Contact Us".

Screenshot from urlscan.io

Cisco Talos Findings

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

The screenshot shows a dark-themed web interface for domain analysis. At the top, there's a search bar with the URL "https://securesupport.vercel.app/" and a magnifying glass icon. Below the search bar are two navigation links: "IP & Domain Reputation Overview" and "Email & Spam Trends".

The main content area is divided into several sections:

- OWNER DETAILS**: Shows the URI (vercel.app/), Hostname (securesupport.vercel.app), Domain (vercel.app), and Network Owner (VERCEL INC).
- REPUTATION DETAILS**: Displays the Web Reputation status as "Untrusted" (indicated by a red cross) and Threat Category as "Malware Exploits" (indicated by a yellow question mark). There's also a button to "Submit Web Reputation Ticket".
- CONTENT DETAILS**: Shows the Content Category as "Computers and Internet" (indicated by a blue question mark). There's a link to "Submit Content Categorization Ticket" and a note about category details being incorrect.
- BLOCK LISTS**: Shows the TALOS SECURITY INTELLIGENCE BLOCK LIST status as "No".

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.

The screenshot shows a web browser window with multiple tabs open. The active tab is a Whois lookup for the domain 'vercel.app' on the Whois.com website. The main content area is divided into two sections: 'Domain Information' and 'Registrar Information'. The 'Domain Information' section shows the following details:

Domain:	vercel.app
Registered On:	2020-01-28
Expires On:	2036-01-28
Updated On:	2026-02-02
Status:	auto renew period client transfer prohibited client update prohibited
Name Servers:	ns1.vercel-dns-3.com ns2.vercel-dns-3.com ns3.vercel-dns-3.com ns4.vercel-dns-3.com

The 'Registrar Information' section shows:

Registrar:	Tucows Domains Inc
IANA ID:	69
Abuse Email:	domainabuse@tucows.com
Abuse Phone:	+1.4165350123

To the right of the main content, there is a sidebar titled 'Interested in similar domains?' with a list of related domains and 'Buy Now' buttons. Below this is a promotional banner for a '.space' domain at \$1.18.

SCREENSHOT FROM WHOIS LOOKUP

6. RISK ASSESSMENT

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