BREAKING CYBERSECURITY NEWS: PHISHERS EXPLOIT GOOGLE SITES AND DKIM REPLAY TO SEND SIGNED EMAILS, STEAL CREDENTIALS

Vairav Cyber Security News Report

Date: April 23, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

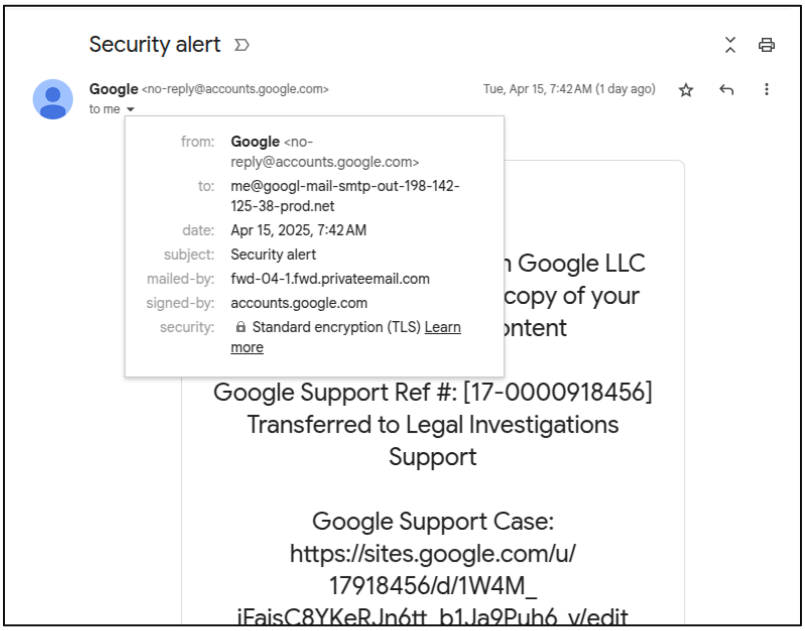
Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A sophisticated phishing campaign has emerged, exploiting Google's own infrastructure to deliver deceptive emails that appear to originate from legitimate Google sources. Attackers are leveraging Google Sites and a technique known as DKIM replay to bypass standard email security protocols, leading to successful credential theft. This method allows malicious emails to pass authentication checks, making them particularly dangerous as they can evade spam filters and appear trustworthy to recipients.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The phishing attack utilizes a DKIM (DomainKeys Identified Mail) replay technique in conjunction with Google Sites to send fraudulent emails that seem authentic. Attackers create a Google OAuth application with a name containing the entire phishing message. When Google sends a security alert about this new app to the attacker's email, the message is signed with a valid DKIM signature. The attacker then forwards this email to the target, preserving the DKIM signature, making it appear as a legitimate message from Google. The email directs recipients to a fake Google Support page hosted on Google Sites, which closely mimics the real site and prompts users to enter their credentials. The suspicious aspect is that, while the "**From**" header suggests the email is from Google, the "**mailed-by**" header points to an unusual mailbox.



Security alert

Google <no-reply@accounts.google.com>
to me

Tue, Apr 15, 7:42 AM (1 day ago)

from: **Google** <no-reply@accounts.google.com>
to: me@googl-mail-smtp-out-198-142-125-38-prod.net
date: Apr 15, 2025, 7:42 AM
subject: Security alert
mailed-by: fwd-04-1.fwd.privateemail.com
signed-by: accounts.google.com
security: 🔒 Standard encryption (TLS) Learn more

n Google LLC
copy of your
ontent

Google Support Ref #: [17-0000918456]
Transferred to Legal Investigations
Support

Google Support Case:
https://sites.google.com/u/
17918456/d/1W4M_
iFaisC8YKeRJn6tt_b1Ja9Puh6_v/edit

Figure 1: Email Headers of the Phishing email

Identification: The attack was identified by Nick Johnson, the lead developer of the Ethereum Name Service (ENS), who received such a phishing email and analyzed its structure. He noted that the email passed all standard authentication checks and was delivered to the inbox without any warnings. Johnson reported the issue to Google, which initially dismissed it but later acknowledged the problem and began implementing countermeasures.

Affected Entities/Industries: This attack affects individual google account holders but it can impact potentially any industry as the attack targets general users.

Potential Impact:

- Unauthorized access to personal and sensitive information
- Credential theft leading to further account compromises
- Potential financial loss and reputational damage

Exploitation Methods:

- DKIM replay attack to bypass email authentication
- Use of Google Sites to host convincing phishing pages
- Spoofed emails appearing to originate from "no-reply@accountgoogle[.]com"

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Enable two-factor authentication (2FA) or passkeys on all accounts
- Verify the authenticity of emails by checking the **mailed-by** email header.
- Avoid clicking on links from unsolicited emails

Security Best Practices

- Educate users about phishing tactics and how to recognize them
- Implement advanced email filtering solutions
- Regularly update and patch systems to protect against known vulnerabilities

For Advanced Security Teams

- Monitor for unusual OAuth application creations and alerts
- Analyze email headers for inconsistencies in DKIM signatures
- Establish protocols for reporting and responding to suspected phishing attempts

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/04/phishers-exploit-google-sites-and-dkim.html

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com