APT group uses fake event invites to phish Google credentials and MFA codes



Researchers describe an APT spear-phishing campaign aimed at people linked to Taiwan research organizations. Victims are sent to an adversary-in-the-middle framework that captures Google credentials and MFA codes.

- The campaign is a spear-phishing operation attributed to an advanced persistent threat actor.
- Targets are individuals affiliated with research organizations in Taiwan.
- Victims are directed to an adversary-in-the-middle (AitM) phishing framework.
- The framework is built to harvest Google account credentials and MFA codes.
- The headline indicates fake event invitations are used as the lure.

What was reported

Researchers have disclosed an APT spear-phishing campaign against individuals affiliated with research organizations in Taiwan. The activity is tracked as UAT-11985, and the reported lure is a fake event invitation.

Victims who follow the lure are sent to an adversary-in-the-middle (AitM) phishing framework. It is designed to capture both Google account credentials and multi-factor authentication codes.

Why it matters for Saudi institutions

The reported targets are in Taiwan, and the source gives no indication of activity in the Kingdom. The technique is still relevant. An AitM page sits between the user and the real login service, so a correct password and a valid one-time code can both be taken in real time. Codes sent by SMS or generated in an app offer limited protection against this method.

Research, academic and policy staff, and executives who regularly receive conference and event invitations, are natural targets for this kind of lure. Cloud email and collaboration accounts that use Google sign-in are the exposed asset.

Recommended posture

Treat unsolicited event invitations that ask for a sign-in as suspect, and review how far your MFA methods resist relay attacks. The source does not list indicators of compromise, so rely on your own monitoring of sign-in activity.

What to do now

1. Remind staff, especially research and executive offices, to verify event invitations through a separate channel before signing in.
2. Assess moving high-risk users to phishing-resistant MFA such as FIDO2 security keys or passkeys.
3. Monitor Google account sign-ins for unusual locations, devices and new sessions, and review alerts promptly.
4. Add AitM phishing to awareness training and simulations, noting that a valid MFA prompt does not prove the site is genuine.
5. Confirm an incident process for suspected credential theft that includes session revocation and password reset.