UAT-11985 Uses Fake Event Invitations in Google AitM Phishing Against Taiwan Research Affiliates



Researchers have disclosed an APT spear-phishing campaign against people tied to Taiwan research organizations. Victims are steered to an adversary-in-the-middle framework that harvests Google credentials and MFA codes.

- The campaign is spear-phishing by an advanced persistent threat actor tracked as UAT-11985.
- Targets are individuals affiliated with research organizations in Taiwan.
- Lures take the form of fake event invitations, per the headline.
- Victims are directed to an adversary-in-the-middle phishing framework.
- The framework is built to capture Google account credentials and MFA codes.

What was reported

Researchers have published details of a spear-phishing campaign attributed to an advanced persistent threat actor tracked as UAT-11985. The activity targets people affiliated with research organizations in Taiwan. According to the report headline, the lure is a fake event invitation.

Victims who follow the link are sent to an adversary-in-the-middle (AitM) phishing framework. It is designed to harvest Google account credentials together with multi-factor authentication (MFA) codes.

Why it matters

AitM frameworks sit between the user and the real sign-in service, so a one-time code typed by the victim can be captured as well as the password. This means that MFA based on codes alone does not fully protect an account against this technique. The source excerpt does not give further technical detail, victim numbers or the full attribution, and we do not speculate beyond it.

Although the campaign is reported against Taiwan, the approach is not tied to one region. Research staff, academics and others who receive event or conference invitations in any country, including Saudi institutions that work with research partners, can be exposed to similar lures.

Practical stance

Treat unsolicited event invitations that ask for a Google sign-in as suspect, and review how far your identity controls resist real-time credential relay. The actions below are proportionate steps for regulated institutions.

What to do now

1. Warn staff, especially those in research, academic and partner-facing roles, about fake event invitations that lead to Google sign-in pages.
2. Where feasible, move privileged and high-risk users to phishing-resistant MFA such as FIDO2 security keys or passkeys instead of code-based MFA.
3. Review email filtering and link-inspection rules for invitation-style messages from unknown senders.
4. Monitor Google Workspace sign-in logs for unusual locations, new devices or sessions following a suspected phishing click.
5. Prepare a clear path for staff to report suspected phishing and to reset credentials and revoke sessions quickly.