



CAMPAIGN PERSWAYSION FOLLOW-UP

Part-2

21 SEP 2026

(U) Executive Summary

Based on a recently published report, CAL-CSIC-202609-T-001.1, The Cal-CSIC has identified additional tactics employed by Cyber Threat Actors (CTAs) who abuse the Microsoft Graph Application Programming Interface (API) in conjunction with passkey-themed social engineering. The CTAs use publicly available information from social media and professional-networking platforms to personalize attacks conducted through phone calls, SMS messages, or Microsoft Teams. To establish persistence, the CTAs register their own phone numbers, authenticator applications, or OTP tokens as an authentication methods for compromised accounts. The CTAs also limit their collection of SharePoint, OneDrive, and email content using Exchange REST APIs to fewer than 1,000 items per hour, spreading the activity across several hours to days to blend in with legitimate activity.

The Cal-CSIC assesses with moderate confidence that these financially motivated threat actors seek to steal data at scale for extortion purposes.

(U) Recommendations:

- Do not engage with those claiming to be IT support if you did not request assistance, especially if they are marked as external
- Employ Phishing-Resistant MFA
- Implement Strict Conditional Access Policies:
 - Block authentication from untrusted locations, or anonymous IPs

(U) Updated TTPs:

- T1684.001 - Social Engineering: Impersonation
 - Impersonation of IT helpdesk to manipulate the victim to make configuration changes
- T1583.001 - Acquire Infrastructure Domains
 - Registers passkey, SSO, and identity-themed domains for phishing operations
- T1556.006 - Modify Authentication Process: Multi-Factor Authentication
 - Attackers registered mobile devices or software OTP for persistence

(U) Reference:

<https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/>

Sharing, Reporting, and Support

Sharing information and intelligence to state, local, federal, and private partners will ensure organizations across California can be better informed and defended.

For questions, concerns, or support or are interested in sharing information or intelligence in any cyber related matter, contact the Cal-CSIC via:

📞 833-REPORT-1 or 916.636.2997

✉️ calcsic@caloes.ca.gov

Report suspicious or suspected foreign activity and incidents to:



Federal Officials at CISA and/or the FBI as applicable



Coordinate with your regional Fusion Center



information, intelligence, and IOCs with ISACs

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and is UNCLASSIFIED//FOR OFFICIAL USE ONLY//TLP:GREEN. Except for TLP: CLEAR, all designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.