



CAMPAIGN PERSWAYSION FOLLOW-UP

11 SEP 2026

(U) Executive Summary

Based on a recently published report, CAL-CSIC-202609-T-001, The Cal-CSIC, along with our partner organization, The California Department of Technology (CDT), have identified additional tactics since at least July 2026. Cyber Threat Actors (CTA) are abusing the Microsoft Graph Application Programming Interface (API) along with "Check My Sign-In" (CMSI) Token Abuse to steal user access tokens. The attackers used this access to obtain additional information from victim assets to further conduct operations. Cal-CSIC assesses with medium confidence that information systems and sensitive institutional data is being targeted for ransomware/extortion by a monetarily motivated CTA.

The Cal-CSIC has recently observed a likely related event where a CTA utilized encrypted emails to obfuscate their activities. This is a likely indication that the CTA may be adopting a new technique to remain unseen on victim networks.

(U) Recommendations:

- Turn on Microsoft Graph Activity Logs via Microsoft Entra ID Diagnostic Settings to stream those logs into your SIEM and/or Microsoft Sentinel
- Collect Entra ID Sign-In and Audit Logs to compare them against unfamiliar authentication data

(U) Threat Hunting

- Lookout for anomalous Sign-In patterns from never-before-seen ASNs, devices, and failed login attempts
- Look for high-frequency "GET" requests targeting the following directories: /users, /groups, /applications, /servicePrincipals, /payroll, /pay, /finance, /HR, /finance, /account, and /admin

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.