EnCyb

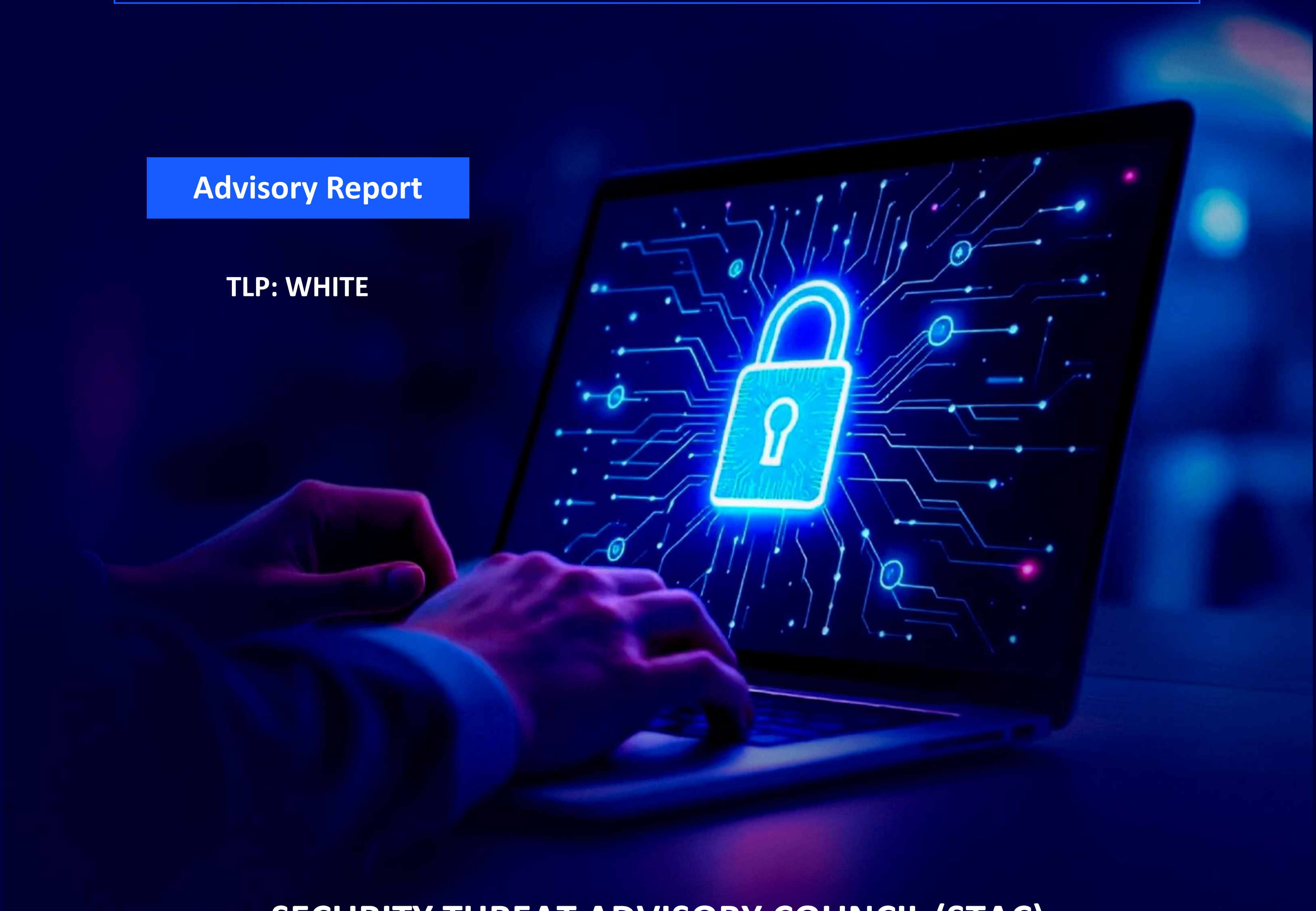
Severity: High

Advisory Type: Threat

macOS RCE via Google Ads Malvertising

Advisory Report

TLP: WHITE



SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Threat actors are abusing Google Search Ads and compromised advertiser accounts to lure macOS users to Apple-lookalike pages that trick them into executing malicious Terminal commands. The campaign results in silent remote code execution, enabling full system compromise including data theft, backdoors, and persistent malware installation.

- Active Region: Global
- Affected Sector: macOS user endpoints in consumer and SMB environments
- Affected Product: macOS (via Google Search Ads / Google Apps Script abuse)
- Severity: High
- Published Date: January 29, 2026

TECHNICAL DETAILS

- **Target:** MacOS end-user systems, specifically user-operated endpoints where individuals perform routine system maintenance tasks and have sufficient privileges to execute shell commands via the Terminal, enabling attacker-controlled code execution under the user's context.

- **Root Cause:** Exploitation of user trust in Google Search Ads and Apple-branded interfaces, combined with social-engineering techniques that trick users into executing obfuscated shell commands, leading to remote code execution.

- **Prerequisite For Exploitation:** The victim must interact with a malicious sponsored search result and manually execute attacker-supplied Terminal commands, typically disguised as legitimate macOS maintenance or cleanup instructions.

IMPACT

- Remote code execution with user-level privileges.
- Installation of persistent malware and backdoors.
- Theft of SSH keys, credentials, and sensitive user data.
- Unauthorized modification of system configurations.
- Deployment of secondary payloads (e.g., crypto-miners, RATs).
- Potential lateral movement within SMB environments.

RECOMMENDATIONS

- Avoid clicking sponsored search results for system utilities or maintenance tools.
- Never copy or execute Terminal commands from unverified websites or ads.
- Use only official Apple documentation or trusted, well-known macOS utilities.
- Enable and enforce macOS security controls such as Gatekeeper, XProtect, and System Integrity Protection (SIP).
- Deploy EDR/XDR solutions to monitor and alert on suspicious shell execution patterns (e.g., curl | bash, base64 -d).
- Enforce MFA on Google Ads and business accounts to reduce the risk of account compromise.

REFERENCE

- https://cybersecuritynews.com/threat-actors-leverage-google-search-ads-for-mac-cleaner/

SECURE, SCALE, SUCCEED WITH CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com