Cybersecurity Report

11.5.2026 – 24.5.2026

Claude Mythos odhalil viac ako 10 000 kritických zraniteľností v široko používanom softvéri

Projekt Glasswing využívajúci model Claude Mythos Preview odhalil počas jedného mesiaca viac ako 10 000 zraniteľností s vysokou a kritickou závažnosťou v široko používanom softvéri vrátane jadra Linuxu, open-source knižníc, vývojárskych nástrojov a ďalších produkčných systémov. AI systém vykonáva autonómnu analýzu zdrojového kódu, identifikuje potenciálne bezpečnostné chyby a generuje dôkazy potrebné na ich validáciu. Nájdené zraniteľnosti zahŕňali chyby umožňujúce vzdialené spustenie kódu, únik citlivých údajov, privilege escalation a ďalšie bezpečnostné nedostatky s reálnym dopadom na bezpečnosť nasadených systémov. Projekt funguje v režime koordinovaného zverejňovania zraniteľností, pričom zistenia sú oznamované maintainerom a dodávateľom ešte pred ich verejným publikovaním.

https://thehackernews.com/2026/05/claude-mythos-ai-finds-10000-high.html

Zmazané Google API kľúče zostávajú aktívne až 23 minút po odstránení

Analýza odhalila, že Google API kľúče môžu aj po odstránení naďalej úspešne autentifikovať požiadavky počas 8 až 23 minút, pričom medián nameraného času bol približne 16 minút. Príčinou je postupná propagácia zmien naprieč infraštruktúrou Google Cloud, v dôsledku čoho niektoré servery odmietajú odstránený kľúč okamžite, zatiaľ čo iné ho naďalej akceptujú. Útočník disponujúci kompromitovaným API kľúčom tak môže počas tohto revokačného okna pokračovať v prístupe k povoleným službám vrátane Gemini API, BigQuery či Google Maps, vykonávať API volania, pristupovať k nahraným súborom alebo exfiltrovať uložené konverzácie. Výskum zároveň poukázal na nepredvídateľné správanie autentifikačnej vrstvy a komplikácie pri incident response, keďže odstránené kľúče sa môžu v telemetrii zobrazovať pod spoločnou kategóriou apikey:UNKNOWN, čo sťažuje atribúciu a sledovanie zneužívania kompromitovaných poverení.

https://cybersecuritynews.com/deleted-google-api-keys-continue-access/

Čínska APT skupina Webworm využíva Discord a Microsoft Graph API pri útokoch na európske vládne organizácie

Skupina Webworm rozšírila svoje operácie na európske vládne inštitúcie a nasadila nové zadné vrátka EchoCreep a GraphWorm. EchoCreep využíva Discord ako C2 kanál, zatiaľ čo GraphWorm komunikuje prostredníctvom Microsoft Graph API a služieb Microsoft 365 vrátane OneDrive, čím sa škodlivá prevádzka maskuje ako legitímna cloudová komunikácia. Útočníci zároveň používajú nástroje ako SoftEther VPN a SOCKS proxy na perzistenciu, tunelovanie prevádzky a obchádzanie detekčných mechanizmov. Kampaň je zameraná na kybernetickú špionáž a zber citlivých informácií z vládnych a verejných organizácií.

https://www.darkreading.com/endpoint-security/chinas-webworm-discord-microsoft-graphs

---

Microsoft upozornil na dve aktívne zneužívané zraniteľnosti v Microsoft Defender

Microsoft zverejnil informácie o dvoch zraniteľnostiach v Microsoft Defender, ktoré sú aktívne zneužívané pri útokoch. Prvá chyba umožňuje lokálnu privilege escalation až na úroveň SYSTEM prostredníctvom nesprávneho spracovania odkazov pri prístupe k súborom, zatiaľ čo druhá môže viesť k denial-of-service stavu a narušeniu funkčnosti bezpečnostného riešenia. Obe zraniteľnosti boli pozorované v reálnych útokoch a podľa dostupných informácií súvisia s verejne známymi exploitmi RedSun a UnDefend, ktoré boli zverejnené ešte pred vydaním opráv. Americká agentúra CISA zaradila obe chyby do katalógu Known Exploited Vulnerabilities (KEV), čo potvrdzuje ich praktické zneužívanie a významné riziko pre organizácie využívajúce Microsoft Defender.

https://thehackernews.com/2026/05/microsoft-warns-of-two-actively.html

---

TeamPCP stojí za rozsiahlymi supply-chain útokmi

Skupina TeamPCP realizuje bezprecedentnú kampaň supply-chain útokov. Útočníci vkladajú infostealer komponenty do legitímnych vývojárskych nástrojov, následne kradnú prístupové tokeny, API kľúče a ďalšie poverenia, ktoré využívajú na kompromitáciu ďalších projektov a CI/CD prostredí. Významným incidentom bolo narušenie interných repozitárov GitHubu po inštalácii škodlivého VS Code rozšírenia zamestnancom spoločnosti, pričom útočníci tvrdia, že získali prístup k približne 3 800 interným repozitárom. Kampaň využíva samoreplikujúci malware Mini Shai-Hulud, ktorý automatizuje šírenie medzi vývojárskymi prostrediami a vytvára reťazec následných kompromitácií naprieč softvérovým dodávateľským reťazcom.

https://www.wired.com/story/teampcp-software-supply-chain-attack-spree-github/