TLP:CLEAR

Prehľad bezpečnostných udalostí csirt.upjs.sk 24.2.2025 – 28.2.2025

Google Cloud KMS pridáva kvantovo bezpečné digitálne podpisy

Google Cloud oznámil podporu kvantovo bezpečných digitálnych podpisov v službe Cloud Key Management Service (Cloud KMS), čím posilňuje ochranu pred budúcimi kvantovými hrozbami. Táto funkcia, dostupná v náhľade, je v súlade s post-kvantovými štandardmi (PQC) od NIST finalizovanými v roku 2024. Umožňuje kvantovo bezpečný import kľúčov, výmenu kľúčov, šifrovanie a digitálne podpisovanie. Google reaguje na hrozbu Harvest Now, Decrypt Later (HNDL), pri ktorej útočníci zbierajú šifrované údaje na budúce dešifrovanie kvantovými počítačmi. Zavedenie zahŕňa algoritmy ML-DSA-65 (FIPS 204) a SLH-DSA-SHA2-128S (FIPS 205) s plánovanou podporou hybridizačných schém.

Lazarus Group ukradla 1,5 miliardy dolárov v kryptomenách

Severokórejská hackerská skupina Lazarus Group vykonala rekordnú kryptomenovú lúpež, keď z burzy Bybit odcudzila približne $1,5 miliardy. Útok sa odohral počas prevodu prostriedkov medzi peňaženkami, kde útočníci manipulovali s procesom podpisovania transakcií. Ukradnuté aktíva zahŕňali 401 347 ETH v hodnote $1,12 miliardy a ďalšie Ethereum tokeny. FBI potvrdila, že Lazarus Group používa falošné obchodné aplikácie na infikovanie zariadení a rýchlo prevádza ukradnuté prostriedky do rôznych kryptomien. Odcudzené financie môžu podporiť severokórejské jadrové programy, čo zvyšuje obavy z kybernetickej kriminality ako geopolitického nástroja.

Google umožnil cielenie reklám na citlivé skupiny používateľov

Investigatíva WIRED odhalila, že Google Display & Video 360 (DV360) umožnil inzerentom cieliť reklamy na používateľov na základe citlivých údajov, ako sú zdravotné stavy, finančné problémy a dokonca zamestnanie v oblasti národnej bezpečnosti. To je v rozpore s pravidlami Googlu, ktorý tvrdí, že takéto cielenie zakazuje. Vyšlo najavo, že dátoví sprostredkovatelia nahrali segmenty obsahujúce informácie o ľuďoch s chronickými ochoreniami či finančnými ťažkosťami. Obzvlášť znepokojivé je zacielenie na amerických vládnych zamestnancov v sektore národnej bezpečnosti, čo predstavuje potenciálne bezpečnostné riziko. Google reagoval tvrdením, že podobné praktiky nepovoľuje, a že podniká kroky proti nevyhovujúcim segmentom, avšak zistenia naznačujú, že kontrolné mechanizmy nie sú dostatočné.

Firefox pokračuje v podpore Manifest V2, zatiaľ čo Chrome zakazuje ad-blockery

Mozilla oznámila, že bude naďalej podporovať Manifest V2, čo umožní používateľom využívať rozšírenia ako uBlock Origin, ktoré Google v Chrome postupne obmedzuje zavedením Manifest V3. Google argumentuje, že nový štandard zvyšuje bezpečnosť, keďže obmedzuje sieťové požiadavky rozšírení, no zároveň znižuje účinnosť blokovania reklám. Mozilla sa však rozhodla zachovať podporu pre staršie rozšírenia, čím si získava priazeň používateľov, ktorí nechcú byť obmedzovaní novými pravidlami Googlu.

Have I Been Pwned pridáva 284 miliónov účtov odcudzených malvérom

Služba Have I Been Pwned (HIBP), známa pre oznamovanie únikov dát, nedávno pridala do svojej databázy viac ako 284 miliónov kompromitovaných účtov. Tieto údaje pochádzajú z 1,5 TB záznamov získaných malvérom na krádež informácií, ktoré boli zdieľané na Telegram kanáli "ALIEN TXTBASE". Tieto záznamy obsahovali 23 miliárd riadkov s 493 miliónmi unikátnych párov webových stránok a e-mailových adries, čo ovplyvnilo 284 miliónov unikátnych e-mailových adries. Okrem toho bolo do HIBP pridaných 244 miliónov nových hesiel, ktoré predtým neboli zaznamenané, a aktualizovaných bolo 199 miliónov už existujúcich hesiel.