TLP: CLEAR

Cybersecurity Report

01.06.2025 - 14.06.2025

Stories

Web3 vývojári čelia vlnám útokov cez open source balíčky

V prostredí kryptomenového a Web3 vývoja prebieha vlna sofistikovaných útokov na open source dodávateľský reťazec, pri ktorých útočníci vkladajú škodlivé balíčky do repozitárov ako npm (75 %) a PyPI (20 %), zamerané najmä na vývojárov pracujúcich s Ethereum, Solana, TRON a TON. Útoky využívajú skripty ako postinstall a setup.py, ktoré spúšťajú škodlivý kód hneď pri inštalácii, aj keď sa balíček nepoužije. Dominujú štyri typy hrozieb: credential stealers, crypto drainers, cryptojackers a clipboard hijackers, pričom najpokročilejšie kampane zachytávajú privátne kľúče priamo počas ich generovania pomocou monkey-patchingu na úrovni knižníc, ako napríklad pri Solana walletoch, kde sú ukradnuté kľúče šifrované cez RSA a skryto odosielané v memo transakciách. Útočníci často využívajú dôveryhodné vývojové nástroje (napr. lintery a validátory), vytvárajú perzistenciu cez startup skripty a cieľovo útočia na cesty ako ~/.config/solana/id.json, čím obchádzajú bežné ochrany vrátane 2FA a hardvérových peňaženiek.

https://cybersecuritynews.com/threat-actors-attacking-cryptocurrency-and-blockchain-developers/

CVE-2025-33053: Kritická RCE zraniteľnosť vo WebDAV zneužívaná APT skupinami

Vážna 0-day zraniteľnosť WebDAV, označená ako CVE-2025-33053, umožňuje vzdialené spustenie kódu (RCE) cez škodlivé .url súbory, ktoré sa automaticky pripájajú na útočníkom riadené WebDAV servery

pri otvorení. Zraniteľnosť vyplýva z nesprávneho spracovania UNC ciest v skratkách a je aktívne zneužívaná v kampaniach proti firemným sieťam, najmä tam, kde beží Apache2 s WebDAV modulmi a slabým prístupovým riadením. Výskumník DevBuiHieu zverejnil funkčný proof-of-concept vrátane skriptov na vytváranie škodlivých .url súborov a nastavenie WebDAV infraštruktúry, čím výrazne zvýšil riziko masového zneužitia.

https://cybersecuritynews.com/webdav-0-day-rce-vulnerability-poc/

BrowserVenom malware zneužíva popularitu DeepSeek-R1 na infikovanie Windows používateľov

Kyberzločinci spustili globálnu kampaň, v ktorej pod zámienkou sťahovania obľúbeného AI modelu DeepSeek-R1 šíria nový malvér BrowserVenom, zameraný na sledovanie sieťovej prevádzky. Útok začína malvertisingom, ktorý falošnú stránku deepseek-platform[.]com zobrazuje na vrchu Google výsledkov. Tá rozpozná používateľov Windows a cez falošné CAPTCHA obrazovky ich navedie na sťahovanie škodlivého súboru AI_Launcher_1.21.exe, ktorý v pozadí inštaluje malvér. Ten presmeruje všetku prehliadačovú komunikáciu cez proxy server 141.105.130[.]106:37121, čím umožňuje odpočúvanie a manipuláciu dát. Kampaň nesie znaky ruského pôvodu a zasiahla používateľov v Latinskej Amerike, Ázii a Afrike, pričom ide o sofistikovaný príklad zneužitia rastúcej popularity AI nástrojov.

https://cybersecuritynews.com/threat-actors-leverages-deepseek-r1-popularity/

Outlook pridáva dvojklik pre šifrované e-maily s cieľom zabrániť nechcenému zobrazeniu citlivých údajov

Od apríla 2025 Microsoft začne zavádzať novú bezpečnostnú funkciu pre Outlook, ktorá vyžaduje dvojklik pri otváraní šifrovaných e-mailov. Používatelia najprv uvidia hlášku „Vaša organizácia vyžaduje kliknutie na ‘Zobraziť správu’“, pričom až následným kliknutím sa obsah e-mailu sprístupní. Funkcia má znížiť riziko náhodného zverejnenia

dôverných údajov počas verejného používania zariadení alebo zdieľania obrazovky. Zavádza sa naprieč platformami – web, desktop aj mobil (iOS, Android) – a bude predvolene vypnutá, no IT správcovia ju môžu aktivovať cez Azure portál alebo PowerShell. Outlook týmto krokom zvyšuje bezpečnostné povedomie používateľov bez výrazného narušenia používateľského zážitku.

https://cybersecuritynews.com/outlooks-two-click-view-encrypted-emails/

Závažná chyba v OpenPGP.js umožňuje falšovanie digitálnych podpisov

Kritická zraniteľnosť (CVE-2025-47934) v knižnici OpenPGP.js umožňuje útočníkom podvrhnúť digitálne podpísané správy a presvedčiť používateľov, že pochádzajú z dôveryhodného zdroja. Chyba sa týka verzií pred v5.11.3 a v6.1.1 a ohrozuje aplikácie, ktoré využívajú túto JavaScriptovú implementáciu pre šifrovanie e-mailov a komunikáciu (napr. Mailvelope). Útočník môže použiť platný podpis z jednej správy a pripojiť k nej škodlivý obsah, ktorý sa následne zobrazí ako overený.

https://cybersecuritynews.com/openpgp-js-vulnerability/
