Cybersecurity Report

26.1.2026 – 8.2.2026

Kompromitované aktualizácie Notepad++ zneužité na šírenie škodlivého kódu

Bezpečnostní výskumníci upozornili na incident, pri ktorom útočníci pravdepodobne napojení na čínsky štát kompromitovali infraštruktúru aktualizácií aplikácie Notepad++ a zneužili ju na šírenie modifikovanej verzie obsahujúcej backdoor, keďže bol škodlivý kód distribuovaný cez legitímny update mechanizmus, útok mal charakter supply-chain kompromitácie a umožňoval nenápadné zavedenie malvéru do systémov používateľov, ktorí dôverovali oficiálnym aktualizáciám, čím sa útočníkom otvorila cesta k vzdialenému prístupu, zberu dát alebo ďalšiemu laterálnemu pohybu v sieti.

https://www.wired.com/story/notepad-plus-plus-china-hackers-update-infrastructure/

Dvojsečná zbraň neľudských identít

Neľudské identity (Non-Human Identities – NHI), ako sú API kľúče, tokeny, servisné účty či workload identity, dnes tvoria základ fungovania cloudových služieb, CI/CD pipeline a automatizovaných procesov, no zároveň predstavujú rastúce bezpečnostné riziko, pretože často majú široké oprávnenia, dlhú životnosť a unikajú tradičnej správe identít. Výskum ukázal tisíce verejne dostupných kontajnerových obrazov obsahujúcich citlivé údaje, napríklad produkčné kľúče alebo cloudové tokeny, čo poukazuje na systémový problém správy tajomstiev v modernom vývoji softvéru. Reálne incidenty, vrátane kompromitácie približne 165 organizácií cez uniknuté prístupové údaje či dlhodobo aktívne GitHub tokeny, demonštrujú, že útočníci čoraz častejšie zneužívajú práve tieto strojové identity namiesto klasických zraniteľností. Na rozdiel od používateľských účtov sa NHI nemenia, „neodchádzajú z firmy“ a často zostávajú aktívne bez rotácie alebo monitoringu, čím sa stávajú perzistentným a ťažko odhaliteľným prístupovým bodom do infraštruktúry. V prostredí cloud-native architektúr tak správa a kontrola neľudských identít predstavuje novú bezpečnostnú hranicu SDLC a vyžaduje rovnaký dohľad, obmedzovanie oprávnení a životného cyklu ako pri ľudských používateľoch.

https://www.bleepingcomputer.com/news/security/the-double-edged-sword-of-non-human-identities/

Semantic Chaining: Nová technika jailbreaku ohrozuje bezpečnost LLM modelov

Výskumníci identifikovali novú techniku označovanú ako *semantic chaining*, ktorá umožňuje obchádzať bezpečnostné mechanizmy veľkých jazykových modelov tým, že škodlivý cieľ rozdelí do série zdanlivo neškodných promptov; namiesto jedného zakázaného dopytu útočník postupne buduje kontext cez viac interakcií, pričom bezpečnostné filtre vyhodnocujú každý krok izolovane a nedokážu rozpoznať kumulatívny zámer, čo umožňuje generovanie obsahu porušujúceho policy alebo vykonávanie nežiaducich úloh. Tento prístup je obzvlášť rizikový pri multimodálnych modeloch, kde môže byť škodlivý obsah rozptýlený medzi text, obrázky alebo iné vstupy, čím sa ešte viac znižuje detekovateľnosť a zvyšuje úspešnosť jailbreaku. Technika poukazuje na zásadnú slabinu súčasných guardrailov – tie sú navrhnuté na detekciu explicitne nebezpečných požiadaviek, no zlyhávajú pri viacfázových, kontextovo distribuovaných útokoch, čo naznačuje potrebu modelov schopných hodnotiť intent naprieč celou konverzačnou históriou a nie iba na úrovni jednotlivých promptov.

https://www.darkreading.com/vulnerabilities-threats/semantic-chaining-jailbreak-gemini-nano-banana-grok-4

Štátom podporovaná kampaň „Shadow Campaigns“ cielila na vlády v 155 krajinách

Štátom podporovaná APT skupina označovaná ako TGR-STA-1030/UNC6619 realizovala rozsiahlu kyberšpionážnu operáciu „Shadow Campaigns“, v rámci ktorej kompromitovala desiatky vládnych a kritických infraštruktúrnych organizácií v 37 krajinách a vykonávala prieskum cieľov až v 155 štátoch, pričom sa zameriavala najmä na ministerstvá, energetiku, financie, diplomaciu či imigračné úrady. Útočníci používali spear-phishing s malvérovým loaderom Diaoyu, ktorý následne nasadzoval nástroje ako Cobalt Strike a VShell, pričom kombinovali tento prístup aj so zneužitím minimálne 15 známych zraniteľností v systémoch vrátane Microsoft Exchange, SAP či sieťových zariadení. Súčasťou kampane bol aj vlastný Linux eBPF rootkit „ShadowGuard“, schopný skrývať procesy a aktivity priamo na úrovni jadra, čo výrazne sťažuje detekciu. Analýza ukazuje, že ide o operatívne vyspelého aktéra orientovaného na strategické, politické a ekonomické spravodajstvo s globálnym dosahom.

https://www.bleepingcomputer.com/news/security/state-actor-targets-155-countries-in-shadow-campaigns-espionage-op/

GlassWorm kampaň zneužíva kompromitované OpenVSX rozšírenia na útoky proti macOS vývojárom

Nová verzia malvéru GlassWorm sa šíri prostredníctvom kompromitovaných rozšírení na platforme OpenVSX, kde útočníci získali prístup k účtu legitímneho vývojára a publikovali trojanizované aktualizácie štyroch populárnych extensionov s viac ako 22 000 stiahnutiami. Po inštalácii sa na macOS nasadí infostealer s perzistenciou cez LaunchAgent, ktorý zbiera citlivé dáta vrátane prihlasovacích údajov z prehliadačov, obsahu macOS Keychain, kryptopeňaženiek a vývojárskych konfigurácií, pričom exfiltrácia prebieha na infraštruktúru útočníka. Kampaň nadväzuje na predchádzajúce vlny GlassWorm a predstavuje typický supply-chain útok zneužívajúci dôveru v legitímne vývojárske nástroje. Prevádzkovateľ platformy odstránil škodlivé balíky a používateľom odporúča preveriť systémy a rotovať kompromitované prihlasovacie údaje.

https://www.bleepingcomputer.com/news/security/new-glassworm-attack-targets-macos-via-compromised-openvsx-extensions/