TLP: CLEAR

Cybersecurity Report

11.08.2025 - 24.08.2025

Stories

Phishing s AI prompt injection

Nová phishingová kampaň maskovaná ako Gmail „Login Expiry Notice“ kombinuje klasickú sociálnu manipuláciu s technikou prompt injection zameranou na AI-založené obranné systémy. Útočníci vložili do HTML kódu emailu skryté inštrukcie určené na zmätok v LLM nástrojoch (ChatGPT, Gemini), ktoré SOC tímy používajú na automatizovanú analýzu. Týmto spôsobom sa snažia dosiahnuť nesprávnu klasifikáciu alebo oneskorenie alertov. Dodávací reťazec obsahoval odoslanie cez SendGrid (SPF/DKIM prešlo, DMARC zlyhalo), prvý hop cez legitímnu Microsoft Dynamics URL, následne CAPTCHA stránku na zablokovanie crawlerov a finálnu phishingovú stránku s Gmail login témou a obfuskovaným JavaScriptom. Okrem krádeže prihlasovacích údajov stránka zbierala IP, ASN a geolokačné údaje a využívala beaconing na odlíšenie reálnych používateľov od botov. Indície z WHOIS a názvov ciest naznačujú možné prepojenie na aktérov z južnej Ázie.

https://cybersecuritynews.com/gmail-phishing-with-prompt-injection/

Docker Desktop SSRF Vulnerability (CVE-2025-9074)

Nová zraniteľnosť CVE-2025-9074 odhalená vo Docker Desktop for Windows (verzie < 4.44.3) umožňuje úplné kompromitovanie hostiteľského systému cez jednoduchý Server-Side Request Forgery (SSRF) útok. Problém spočíva v tom, že Docker sprístupňuje interný HTTP API endpoint na http://192.168.65.7:2375/ bez akejkoľvek autentifikácie, čo umožňuje ľubovoľnému kontajneru vytvárať a

spúšťať privilegované kontajnery s pripojením hostiteľského súborového systému. Exploit vyžaduje iba dva HTTP POST requesty – prvý vytvorí kontajner s mountom Windows C: disku na /host_root, druhý ho spustí – čím útočník získa prístup na úrovni administrátora. Keďže útok možno realizovať aj cez SSRF z kompromitovaných webových aplikácií, nejde len o lokálne riziko. Podobný problém bol nezávisle identifikovaný aj na macOS. Docker vydal verziu 4.44.3, ktorá zavádza autentifikáciu a lepšiu segmentáciu medzi workloadmi a control plane, pričom pre zraniteľné systémy neexistuje žiadny iný workaround.

https://cybersecuritynews.com/windows-docker-desktop-vulnerability/

Bankový trójsky kôň Anatsa (TeaBot) spustil globálne kampane

Bankový trójsky kôň Anatsa, známy aj ako TeaBot, patrí medzi najpokročilejšie hrozby pre Android a v roku 2025 cieli už na viac než 831 finančných inštitúcií a kryptomenové platformy naprieč viacerými kontinentmi vrátane Nemecka a Južnej Kórey. Malvér sa šíri priamo cez Google Play Store, kde sa maskuje ako legitímne aplikácie na čítanie dokumentov alebo správu súborov, pričom po inštalácii stiahne škodlivý payload zo vzdialeného C2 servera. Nová verzia nahradila dynamické načítavanie DEX súborov priamou inštaláciou hlavného malvéru a implementuje pokročilé techniky na obchádzanie analýzy: runtime DES dešifrovanie reťazcov, použitie poškodených ZIP archívov na skrytie DEX súborov a získavanie práv cez Accessibility Services. Pre komunikáciu s operátormi využíva XOR šifrovanie a viacero C2 domén čím si zabezpečuje redundanciu a perzistenciu.

https://cybersecuritynews.com/anatsa-malware-attacking-android-devices/

Zraniteľnosť v Azure umožnila prístup k cudzím účtom a službám

V systéme Microsoft Azure bola objavená vážna bezpečnostná chyba, ktorá umožňovala útočníkom získať prístup k citlivým zdrojom iných

organizácií, vrátane Key Vaults, databáz Azure SQL či služieb ako Jira a Salesforce. Problém súvisel s tým, že všetky API pripojenia boli spracovávané na jednej zdieľanej infraštruktúre, čo narušilo oddelenie jednotlivých zákazníkov. Výskumník Gulbrandsrud ukázal, že zneužitím špeciálneho požiadavku sa dalo preniknúť do cudzích pripojení a získať ich oprávnenia. Microsoft reagoval rýchlo – do troch dní chybu potvrdil, do týždňa nasadil opravy a výskumníkovi vyplatil odmenu 40 000 USD. Aj keď útok vyžadoval určité oprávnenia v rámci vlastného účtu, rozsah problému bol kritický, keďže narúšal základný princíp bezpečného oddelenia zákazníkov v cloudových službách.

https://cybersecuritynews.com/azures-default-api-connection-vulnerability/

Firefox 142 opravuje kritické zraniteľnosti umožňujúce vzdialené spustenie kódu

Mozilla vydala verziu Firefox 142, ktorá rieši viacero vysoko závažných zraniteľností ohrozujúcich používateľov na rôznych platformách. Medzi najkritickejšie patrí chyba v sandboxe multimediálneho modulu, ktorá môže viesť k úniku z izolovaného prostredia a spusteniu škodlivého kódu, ako aj zraniteľnosti v grafickom engine a pamäťové chyby umožňujúce remote code execution. Výskumníci zároveň upozornili, že niektoré chyby zasahujú aj Extended Support Release (ESR) verzie používané vo firemných prostrediach, čím zvyšujú riziko pre podnikové siete. Aktualizácia na najnovšiu verziu Firefoxu je preto nevyhnutná, keďže útoky by mohli viesť k úplnému prevzatiu systému pri návšteve škodlivých webových stránok.

https://cybersecuritynews.com/mozilla-high-severity-vulnerabilities/
