Cybersecurity Report

5.11.2025 – 12.11.2025

Stories

GlassWorm sa vracia a zaoberá sa rozšíreniami VS kódu

Malvér GlassWorm, ktorý infikuje vývojárske stanice prostredníctvom rozšírení pre Visual Studio Code (VS Code), sa opäť objavil, pričom jeho kampane infikovali podľa výskumníkov vyše 35 000 strojov v globálnom meradle. Malvér sa šíri cez repositáre Open VSX (a čiastočne aj cez oficiálny VS Code Marketplace), pričom útočníci využívajú "neviditeľné" Unicode znaky v kóde, ktoré sa síce zobrazia v editore ako prázdny priestor, no skrývajú škodlivé funkcie. GlassWorm po infikovaní ukradne vývojárske údaje (napr. GitHub / npm / OpenVSX tokeny), zriadi proxy siete zo strojov obetí, a ako C2 infraštruktúru využíva napríklad blockchain Solana či kalendár Google. Útok poukazuje na rastúce riziko supply-chain kompromitácií v prostredí vývoja softvéru, kde vývojárske stanice môžu slúžiť ako odrazový mostík pre rozsiahlejsie incidenty v organizáciách.

https://www.darkreading.com/cyberattacks-data-breaches/glassworm-returns-vs-code-extensions

---

Microsoft opravil 63 bezpečnostných chýb vrátane aktívneho zero-day na jadro Windows

Spoločnosť Microsoft vydala novemberové bezpečnostné aktualizácie, ktoré riešia 63 zraniteľností – z toho 4 kritické a 59 dôležitých. Medzi nimi je jedna aktuálne zneužívaná zero-day chyba (CVE-2025-62215) v jadre Windows, ktorá útočníkom umožňuje eskaláciu práv na úroveň SYSTEM. Okrem toho obsahuje súbor záplat aj chyby umožňujúce vzdialené spustenie kódu (RCE), únik informácií a obchádzanie bezpečnostných opatrení. Pre organizácie je kľúčové obratom nasadiť tieto záplaty, najmä ak používajú podporované verzie Windows, a venovať zvýšenú pozornosť komponentom ako jadro OS a grafické knižnice.

https://thehackernews.com/2025/11/microsoft-fixes-63-security-flaws.html

---

Viaceré zraniteľnosti v ChatGPT umožňujú masívne úniky dát

Tenable odhalil sedem vážnych zraniteľností v ChatGPT aj SearchGPT, ktoré útočníkom umožňujú rôzne formy indirektnej prompt-injekcie, neoprávnený prístup k dátam používateľov a manipuláciu správania modelu. (darkreading.com) Výskumníci ukázali, že škodlivý obsah vložený na web, do komentárov alebo generovaný URL adresou môže prinútiť ChatGPT ignorovať interné bezpečnostné pravidlá, prezradiť uložené „memórie“, prepísať pokyny používateľa alebo dokonca vykonávať akcie v mene obete. Viaceré útoky fungovali ako „zero-click“, stačilo aby model spracoval škodlivý text počas vyhľadávania či sumarizácie. Problémy zasahujú aj profesionálne prostredia, kde ChatGPT pracuje s citlivými firemnými dokumentmi, čím vzniká riziko exfiltrácie interných dát. OpenAI potvrdilo, že časť zraniteľností už opravilo, no výskum ukazuje, že LLM systémy trpia systémovými slabinami v oblasti izolácie vstupov, validácie kontextu a ochrany pred prompt-injekciou.

https://www.darkreading.com/application-security/multiple-chatgpt-security-bugs-rampant-data-theft

---

GootLoader využíva nový trik so špeciálnymi fontmi na infikovanie stránok WordPress

Malvér GootLoader, ktorý bol tento rok na určitý čas potlačený, sa opäť objavil a tentoraz používa inovatívnu metódu obfuskácie — na kompromitovaných WordPress stránkach útočníci nasadili vlastné WOFF2 webové fonty, ktoré skryjú skutočné názvy súborov a download odkazy v HTML zdroji. Vírusové domény zverejnili tisíce klamlivých stránok so šablónami právnych dokumentov, ktoré sa vo výsledku zobrazujú legitímne, ale vedú k stiahnutiu škodlivého skriptu (.JS), ktorý infikuje systém a často vedie k ransomvérovému útoku. V niektorých prípadoch došlo k plnému prevzatiu riadenia doménového kontroléra už do 17 hodín od infekcie. Obrana vyžaduje zvýšenú pozornosť na stiahnuté súbory z webu, monitoring neobvyklého JavaScriptu a kontrolu fontov alebo vzhľadu textu na webových stránkach.

https://thehackernews.com/2025/11/gootloader-is-back-using-new-font-trick.html

---

WhatsApp screen-sharing podvod

Podvodná kampaň zneužíva funkciu zdieľania obrazovky v aplikácii WhatsApp: útočník zahájí videohovor s obeťou, predstiera dôveru (napr. banka alebo známy), vyvolá paniku kvôli údajnému problému a následne požiada o zdieľanie obrazovky alebo inštaláciu nástrojov na vzdialený prístup, čím získa plný prístup ku kredenciálom, OTP či bankovým aplikáciám. Prípady boli zaznamenané vo Veľkej Británii, Indii i Hong Konge, kde napríklad obeť prišla o 700 000 USD. Útok stavia na dôveru, urgentnosť a neustálu kontrolu používateľa pod zámienkou pomoci, pričom technická bariéra je nízka – postačí stlačenie tlačidla „Zdieľať".

https://www.welivesecurity.com/en/scams/sharing-is-scaring-whatsapp-screen-sharing-scam/