TLP: CLEAR

Cybersecurity Report

05.05.2025 - 18.05.2025

Stories

Sofistikovaný NPM Attack využíva Google Calendar C2 na sofistikovanú komunikáciu

Výskumníci z Veracode odhalili pokročilý supply chain útok na NPM, v ktorom malvér komunikuje cez Google Kalendár. Škodlivý kód bol ukrytý v legitímne vyzerajúcich JavaScriptových knižniciach, ktoré po inštalácii využívajú OAuth tokeny na prístup k API, vytvárajú kalendárové udalosti s príkazmi v popisoch a pravidelne ich čítajú. Malvér sa tak skryje v bežnej prevádzke a dokáže spúšťať kód, kradnúť dáta či sťahovať ďalší malvér. Infikované balíčky boli stiahnuté vyše 35 000-krát. Obsahuje techniky na obídenie analýzy a nespúšťa sa v sandboxe. Odborníci odporúčajú monitorovanie OAuth prístupov, kontrolu závislostí a detekciu podozrivého používania Google API.

https://cybersecuritynews.com/sophisticated-npm-attack-exploits-google-calendar-c2/

Súd EÚ rozhodol, že sledovacie reklamy porušujú GDPR

Odvolací súd v Bruseli rozhodol, že sledovanie používateľov na účely cielených reklám – vrátane tzv. real-time bidding – je v rozpore s Všeobecným nariadením o ochrane údajov (GDPR) pre nedostatočný systém súhlasu. Súd označil široko používaný rámec Transparency and Consent Framework za nevyhovujúci, čím spochybnil právny základ, na ktorom stojí cielená reklama veľkých technologických firiem ako Google, Amazon, Microsoft a X. Podľa Amnesty International bežné vyskakovacie okná na získanie súhlasu nezabraňujú vážnemu narušeniu súkromia, keďže údaje používateľov

sa zdieľajú s tisíckami firiem bez dostatočnej kontroly. Systém real-time bidding, ktorý v reálnom čase draží reklamný priestor na základe správania používateľov a obsahu stránky, bol označený za vážne porušenie súkromia. Amnesty rozhodnutie označila za veľké víťazstvo digitálnych práv a vyzvala technologický sektor, aby prešiel na modely reklamy, ktoré rešpektujú súkromie používateľov.

https://therecord.media/eu-court-rules-tracking-based-ads-illegal

---

Nová zraniteľnosť sa týka všetkých procesorov Intel za posledných 6 rokov

Výskumníci z ETH Zurich odhalili novú zraniteľnosť BPRC (Branch Predictor Race Conditions), ktorá postihuje všetky Intel procesory z posledných šiestich rokov. Využíva chybu v spekulatívnom vykonávaní, pri ktorej útočník môže počas prepínania oprávnení krátkodobo získať prístup do cudzej pamäte a kradnúť dáta rýchlosťou vyše 5 000 bajtov za sekundu. Hrozí najmä v cloudových prostrediach, kde viacero používateľov zdieľa rovnaký hardvér. Zraniteľnosť sa podobá na predchádzajúce útoky ako Spectre či Retbleed. Intel vydal opravy v roku 2024, no ide len o dočasné riešenia s dopadom na výkon. Trvalá ochrana si vyžaduje zmeny v architektúre procesorov. Odborníci odporúčajú aktualizovať mikrokód, firmvér, OS a sledovať anomálie v správaní cache.

https://cybersecuritynews.com/new-vulnerability-affects-all-intel-processors/

Hackeri zamaskovali malvér pre vzdialený prístup ako službu Microsoft Edge

Výskumníci odhalili kampaň, v ktorej bol MeshCentral agent zamaskovaný ako legitímna služba Microsoft Edge pod cestou C:\Program Files\Microsoft\MicrosoftEdge\msedge.exe. Ako ukázalo vyšetrovanie Stephena Bergera, útočníci využili názvy a adresáre podobné originálnym súborom Windows, aby ukryli vysoko privilegovaný vzdialený prístup. Agent komunikoval cez porty 80 a 443, prežil reštarty aj núdzový režim, a každý inštančný súbor bol

jedinečný, čo sťažilo detekciu. Incident ukázal, že viditeľnosť v sieti a na koncových bodoch je kľúčová pre rýchlu reakciu a odhalenie takto skrytých hrozieb.

https://cybersecuritynews.com/remote-access-malware-as-microsoft-edge/

Bitpixie: Kritická zraniteľnosť BitLockeru umožňuje obísť šifrovanie za menej než 5 minút

Zraniteľnosť CVE-2023-21563, nazývaná Bitpixie, umožňuje softvérový útok na BitLocker bez potreby fyzického zásahu, pričom dokáže získať Volume Master Key (VMK) priamo z pamäte po PXE reštarte. Chyba v Windows bootloaderi spôsobí, že VMK nie je po zlyhaní bootovania z pamäte vymazaný. Výskumníci ukázali dva postupy: Linux verzia načíta vlastné jadro a získa VMK cez kernel modul; Windows PE verzia používa iba Microsoft-podpísané komponenty a nástroj WinPmem. Obe metódy fungujú len ak nie je zapnutá pre-boot autentifikácia (PIN, USB kľúč). Verejne dostupný PoC skript umožňuje automatizovať útok do 5 minút.

https://cybersecuritynews.com/bitlocker-encryption-bypassed/
