Cybersecurity Report

26.4.2026 - 10.5.2026

Hacknuteľné robotické kosačky ukazujú rastúce riziká IoT zariadení

Bezpečnostní výskumníci odhalili kritické zraniteľnosti v robotických kosačkách Yarbo, ktoré umožňovali vzdialené prevzatie zariadenia, prístup ku kamerám, GPS polohe či dokonca Wi-Fi heslám používateľov. Problém spôsobovali hardcoded prihlasovacie údaje a vzdialené diagnostické backdoory, ktoré mohli útočníci zneužiť na ovládanie tisícov zariadení po celom svete. Incident poukazuje na rastúce bezpečnostné riziká IoT a smart home technológií, kde zlyhanie bezpečnosti môže mať nielen dopad na súkromie, ale aj fyzickú bezpečnosť používateľov. Výrobca po zverejnení chýb prisľúbil bezpečnostné aktualizácie a odstránenie problematických mechanizmov vzdialeného prístupu.

https://www.wired.com/story/security-news-this-week-hackable-robot-lawnmower-unlocks-a-new-nightmare/

CLBanker zneužíva WhatsApp a Outlook na automatické šírenie bankového malvéru

Výskumníci odhalili nový brazílsky bankový trójsky kôň TCLBanker, ktorý sa šíri cez trojanizovaný Logitech AI installer a následne zneužíva účty používateľov vo WhatsApp Web a Microsoft Outlook na automatické rozposielanie phishingových správ a škodlivých súborov. Malvér cieli na desiatky bankových, fintech a kryptomenových platforiem, pričom využíva overlay techniky na krádež prihlasovacích údajov a vzdialené ovládanie zariadenia. Súčasťou kampane sú aj anti-analysis mechanizmy, DLL sideloading a schopnosť obchádzať tradičné emailové filtre tým, že správy odosiela priamo z kompromitovaných účtov obetí.

https://cybersecuritynews.com/tclbanker-malware-targets-users-whatsapp-outlook-worm-modules

Škoda potvrdila bezpečnostný incident po útoku na online obchod

Automobilka Škoda Auto oznámila bezpečnostný incident, pri ktorom útočníci zneužili zraniteľnosť v softvéri jej online obchodu a získali neoprávnený prístup k zákazníckym dátam. Kompromitované mohli byť mená, adresy, emaily, telefónne čísla, informácie o objednávkach a hashované heslá používateľských účtov, pričom platobné údaje údajne zasiahnuté neboli. Po odhalení incidentu spoločnosť dočasne odstavila e-shop, opravila zraniteľnosť a zapojila externých forenzných expertov do vyšetrovania. Rozsah prípadného exfiltrácie dát zatiaľ nebol potvrdený.

https://cybersecuritynews.com/skoda-security-incident/

Hackeri zneužívajú falošné inštalačné stránky Claude AI na šírenie malvéru

Bezpečnostní výskumníci odhalili kampaň, pri ktorej útočníci vytvárajú falošné inštalačné stránky pre Claude AI, ktoré sa vizuálne podobajú oficiálnym zdrojom a sú šírené aj cez reklamy vo vyhľadávačoch. Po stiahnutí údajného inštalačného balíka používateľ získa legitímne vyzerajúcu aplikáciu, no v pozadí sa aktivuje škodlivý reťazec (napr. skripty alebo DLL sideloading), ktorý inštaluje infostealery alebo vzdialené prístupy. Útočníci cielia najmä na používateľov, ktorí hľadajú AI nástroje a dôverujú „one-click" inštalačným postupom, čím získavajú prístup k heslám, cookies a systémovým dátam. Kampaň je súčasťou širšieho trendu zneužívania popularity AI platforiem na distribúciu malvéru.

https://cybersecuritynews.com/hackers-using-fake-claude-ai-installer-pages/

PyPI balíky šírili ZiChatBot malware cez Zulip API a infostealer komponenty

Bezpečnostní výskumníci odhalili tri škodlivé balíky na Python Package Index (PyPI), ktoré sa vydávali za legitímne knižnice, ale po nainštalovaní potichu doručovali malware rodiny ZiChatBot na Windows aj Linux systémoch. Balíky fungovali ako droppery, ktoré po spustení načítali ďalšie škodlivé komponenty a využívali Zulip API ako C2 (command-and-control) kanál na skrytú komunikáciu s útočníkmi. Súčasťou kampane bolo aj kradnutie prihlasovacích údajov, systémových tokenov a citlivých dát z vývojárskych prostredí, pričom útok cielil najmä na vývojárov a CI/CD reťazce. Incident je ďalším príkladom softvérovej supply-chain kompromitácie v open-source ekosystéme.

https://thehackernews.com/2026/05/pypi-packages-deliver-zichatbot-malware.html