Cybersecurity Report

25.5.2026 – 7.6.2026

Zraniteľnosť v Microsoft Edge umožňuje vzdialené spustenie kódu

Microsoft vydal bezpečnostnú opravu pre zraniteľnosť v prehliadači Microsoft Edge, ktorú môže vzdialený útočník zneužiť na spustenie ľubovoľného kódu v kontexte používateľa po otvorení špeciálne vytvoreného webového obsahu. Chyba ovplyvňuje Chromium-based verzie Edge a jej úspešné zneužitie môže viesť ku kompromitácii systému, obchádzaniu bezpečnostných obmedzení a manipulácii s dátami. Zraniteľnosť predstavuje významné riziko najmä pri phishingových kampaniach a drive-by útokoch, kde stačí interakcia používateľa s podvrhnutou webovou stránkou.

https://cybersecuritynews.com/microsoft-edge-vulnerability-code-execution/

Kampaň FlutterBridge šíri backdoor FlutterShell na macOS cez škodlivé reklamy

Útočníci v rámci kampane FlutterBridge distribuujú nový macOS backdoor FlutterShell prostredníctvom škodlivých reklám v Google Search a na YouTube, ktoré používateľov presmerovávajú na falošné stránky napodobňujúce legitímny softvér. FlutterShell je vytvorený vo frameworku Flutter a okrem adware funkcionality poskytuje útočníkom plnohodnotný vzdialený prístup vrátane spúšťania shell príkazov, manipulácie so súbormi a exfiltrácie dát. Malvér využíva architektúru založenú na WebView, pričom škodlivá logika je hostovaná na vzdialených serveroch a môže byť dynamicky menená bez potreby aktualizácie binárky. Niektoré varianty zároveň zneužívajú AI sumarizačné funkcie na odosielanie dokumentov cez infraštruktúru kontrolovanú útočníkmi pred ich spracovaním, čím rozširujú možnosti krádeže citlivých údajov.

https://thehackernews.com/2026/06/fluttershell-backdoor-spreads-to-macos.html

Útočníci zneužívajú Microsoft Teams a Google Drive na šírenie Nimbus RAT

Útočníci vedú viacstupňovú sociálno-inžiniersku kampaň, v ktorej kombinujú email bombing, impersonáciu IT podpory cez Microsoft Teams a zneužitie nástroja Quick Assist na získanie vzdialeného prístupu k systémom obetí. Po úspešnom prístupe nasadzujú Java-based malware Nimbus RAT, ktorý poskytuje vzdialené ovládanie zariadenia, krádež prihlasovacích údajov a spúšťanie dodatočného škodlivého kódu. Malvér využíva Google Drive a Google Sheets ako C2 infraštruktúru a kanál na exfiltráciu dát, čím maskuje komunikáciu ako legitímnu prevádzku voči

dôveryhodným cloudovým službám. Kampaň je zameraná na podnikové prostredia a demonštruje rastúci trend zneužívania kolaboračných a cloudových platforiem na získanie počiatočného prístupu a následnú kompromitáciu organizácií.

https://cybersecuritynews.com/microsoft-teams-and-google-drive-abused/

Detské údaje predstavujú rastúci cieľ krádeže identity a syntetických podvodov

Deti sa stávajú čoraz atraktívnejším cieľom pre útočníkov, keďže ich osobné údaje majú dlhú životnosť a často nie sú roky monitorované. Kompromitované údaje zo školských systémov, herných platforiem, zdravotných záznamov či online služieb môžu byť zneužité na krádež identity alebo vytváranie syntetických identít používaných pri finančných podvodoch. Riziko zvyšuje rastúci objem osobných informácií zdieľaných rodičmi na sociálnych sieťach, časté úniky dát v sektore vzdelávania a zdravotníctva a používanie AI služieb, do ktorých deti vkladajú citlivé údaje bez pochopenia bezpečnostných dôsledkov. Podľa údajov FTC vzrástol počet prípadov krádeže identity detí medzi rokmi 2021 a 2024 o 40 %, pričom zneužitie býva často odhalené až po rokoch pri zakladaní bankových účtov, žiadostiach o úver alebo iných finančných operáciách.

https://www.welivesecurity.com/en/kids-online/lessons-life-childrens-data-long-term-identity-risk/

Android zavádza overovanie identity volajúcich proti AI hlasovým podvodom

Google predstavil funkciu Fake Call Detection, ktorá má chrániť používateľov Androidu pred podvodnými hovormi využívajúcimi spoofing telefónnych čísel a AI generované hlasové klony. Mechanizmus je integrovaný do aplikácie Phone by Google a pomocou šifrovaného RCS kanála overuje, či hovor skutočne pochádza zo zariadenia kontaktu, ktorého identita sa zobrazuje na obrazovke. Ak overenie zlyhá, systém upozorní používateľa na možný impersonation útok a označí hovor ako podozrivý. Funkcia cieli najmä na rastúci trend sociálno-inžinierskych kampaní, v ktorých útočníci kombinujú spoofing telefónnych čísel s AI voice cloning technológiami na presvedčivé vydávanie sa za dôveryhodné osoby.

https://www.wired.com/story/android-is-fighting-phone-scams-with-a-new-feature-to-prove-whos-calling/