TLP: CLEAR

Cybersecurity Report

25.11.2025 - 27.11.2025

Stories

CISA varuje pred aktívnymi útokmi na používateľov populárnych chatovacích aplikácií

CISA upozornila, že útočníci aktuálne zneužívajú komerčný spyware a RAT nástroje na útoky proti používateľom mobilných messengerov, pričom využívajú sociálne inžinierstvo, QR kódy na prepojenie zariadení, zero-click exploity aj falošné verzie aplikácií. Kampane zahŕňajú únosy Signal účtov cez funkciu „linked devices“, špionážne appky ProSpy/ToSpy v SAE, ClayRat šírený cez Telegram kanály, reťazenie zraniteľností v iOS a WhatsApp (CVE-2025-43300, CVE-2025-55177) či zneužitie Samsung chyby (CVE-2025-21042) na doručenie spyware LANDFALL. Útoky cielia najmä na vysokohodnotné osoby – vládnych a vojenských predstaviteľov, politikov a občianske organizácie v USA, Európe a na Blízkom východe. CISA odporúča používať E2EE komunikáciu, FIDO autentifikáciu, vyhnúť sa SMS-MFA, pravidelne aktualizovať, obmedziť povolenia aplikácií a využívať bezpečnostné funkcie moderných Android a iOS zariadení.

https://thehackernews.com/2025/11/cisa-warns-of-active-spyware-campaigns.html

---

Microsoft Teams: Cross-tenant slabina umožňuje obísť Defender ochrany cez guest prístup

Výskumníci upozorňujú na významnú slabinu v Microsoft Teams, ktorá útočníkom umožňuje obísť ochrany Microsoft Defender for Office 365 využitím guest prístupu do externých tenantov. Keď používateľ prijme pozvánku na chat ako „guest“ v inom tenante, riadia sa jeho ochrany výhradne bezpečnostnými politikami hostiteľského prostredia, nie

jeho vlastnej organizácie. To znamená, že ak útočník vytvorí vlastný Microsoft 365 tenant bez bezpečnostných prvkov (napr. lacné licencie bez Defenderu), môže pozývať obete do „protection-free zones“ a následná komunikácia prebieha bez kontrol ako Safe Links či Safe Attachments. Pozvánky pochádzajú z infraštruktúry Microsoftu, takže prejdú SPF/DKIM/DMARC a typické e-mailové filtre ich neoznačia ako rizikové. Po prijatí pozvánky môže útočník posielať phishingové odkazy alebo malvérové súbory bez toho, aby to organizácia obete videla.

https://thehackernews.com/2025/11/ms-teams-guest-access-can-remove.html

---

Microsoft sprísni bezpečnosť Entra ID: blokovanie script injection pri prihlasovaní od roku 2026

Microsoft plánuje od októbra 2026 sprísniť Content Security Policy (CSP) pre Entra ID prihlasovanie na login.microsoftonline.com, aby zastavil neautorizované script injection útoky. Nové pravidlá povolia spúšťanie len skriptov z dôveryhodných Microsoft domén a blokujú všetok injektovaný alebo externý kód, čím znižujú riziko XSS útokov počas autentifikácie. Zmeny sa týkajú len webového prihlasovania, nie Entra External ID. Firmy majú vopred otestovať svoje prihlasovacie toky a vyhnúť sa nástrojom a rozšíreniam, ktoré do login stránky vkladajú skripty. CSP porušenia možno odhaliť priamo v developer console pri chybách „Refused to load the script“. Úprava je súčasťou Microsoft Secure Future Initiative, ide o snahu blokovať útoky už pri autentifikácii a priblížiť sa k plnému Zero Trust prístupu.

https://thehackernews.com/2025/11/microsoft-to-block-unauthorized-scripts.html

---

Kyberútoky na influencerov: rastúce riziko pre účty a sledovateľov

Influenceri sú čoraz častejším cieľom kyberzločincov, ktorí zneužívajú ich veľké publikum, dôveru sledovateľov a často slabé zabezpečenie účtov. Útočníci používajú spear-phishing, credential stuffing, SIM swapping a AI na personalizované útoky, aby prevzali kontrolu nad

účtom, šírili podvody, malware či crypto scamy, vydierali tvorcov alebo kradli kontakty followerov. Napadnutý účet môže spôsobiť finančné straty, poškodiť reputáciu influencera aj značiek a umožniť priame podvody na e-shopoch.

https://www.welivesecurity.com/en/social-media/influencers-crosshairs-cybercriminals-targeting-content-creators/

Nový Android malware Sturnus ohrozuje šifrované správy a bankové účty

Výskumníci odhalili nový Android banking trojan s názvom Sturnus, ktorý dokáže zachytávať správy z aplikácií ako WhatsApp, Telegram či Signal po ich dešifrovaní a kradnúť bankové prihlasovacie údaje cez presvedčivé falošné prihlasovacie obrazovky. Malware umožňuje útočníkom takmer úplnú kontrolu nad zariadením – sleduje kontakty, celé správy, vloží text, sleduje aktivitu používateľa a vykonáva transakcie cez čiernu obrazovku, ktorá skrýva jeho činnosť. Sturnus je zatiaľ v obmedzenom testovaní a zameriava sa na banky v Strednej a Južnej Európe, čo naznačuje prípravu na širšiu kampaň. Malware patrí do novej vlny sofistikovaných Android trojanov, ktoré cieľovo ohrozujú finančné aplikácie a používateľov vysokej hodnoty.

https://therecord.media/new-android-malware-captures-private-messages

---