# Cybersecurity Report

## 12.1.2026 – 25.1.2026

---

### Masívny data breach 149 miliónov prihlasovacích údajov vrátane Gmail a Facebook

Bezpečnostný analytik Jeremiah Fowler objavil nezabezpečenú databázu obsahujúcu 149 miliónov unikátnych používateľských mien a hesiel pre širokú škálu online služieb, ktoré boli public-accessible bez akéhokoľvek šifrovania či hesla. Medzi kompromitovanými údajmi bolo približne 48 mil. Gmail účtov, 17 mil. Facebook účtov a 420 000 Binance účtov, ako aj prihlasovacie údaje pre Yahoo, Outlook, iCloud, .edu akademické účty, TikTok, Netflix a dokonca údaje súvisiace s vládnymi systémami viacerých krajín, čo predstavuje vážnu hrozbu pre súkromie a bezpečnosť používateľov. Fowler predpokladá, že tento obrovský súbor vznikol z automatizovaného zberu pomocou infostealer malvéru, ktorý zachytáva poverenia z infikovaných zariadení, vrátane keylogger techník, a ukladá ich do prehľadnej databázy, ktorá počas takmer mesiaca zostala prístupná verejne, kým ju hosting providera nakoniec nezablokoval.

https://www.wired.com/story/149-million-stolen-usernames-passwords/

---

### Microsoft Teams prinesie External Domains Anomalies Report na detekciu podozrivej komunikácie

Microsoft pripravuje novú bezpečnostnú funkciu pre Teams, ktorá v februári 2026 začne generovať External Domains Anomalies Report — report o anomáliách v komunikácii s externými doménami určený pre IT administrátorov. Tento nástroj analyzuje vzorce komunikácie, vytvára baseline „normálneho“ správania a upozorňuje na odchýlky ako náhle nárasty správ, prvé interakcie s neznámymi doménami alebo neobvyklé engagement vzory, ktoré môžu signalizovať rizikové aktivity, sociálne inžinierstvo alebo potenciálne kompromitácie predtým, než vyúste do úniku dát či iného incidentu.

https://cybersecuritynews.com/microsoft-teams-external-domain-anomalies/

---

### Nasadenia súkromných koncových bodov Azure vystavujú zdroje Azure útoku DoS

Nesprávne nastavené Azure Private Endpoints môžu neúmyselne odhaliť interné cloudové zdroje, ktoré mali byť dostupné iba v rámci privátnej siete. Problém vzniká najmä pri chybnej DNS konfigurácii alebo nedostatočných sieťových obmedzeniach, čo môže umožniť útočníkom identifikovať a potenciálne osloviť služby ako Storage Accounts, databázy či App Services. Nejde o chybu v samotnom Azure, ale o riziko vyplývajúce zo slabej implementácie bezpečnostných kontrol, preto je dôležité pravidelne kontrolovať sieťové politiky, prístupové pravidlá a monitorovať konfiguráciu privátnych endpointov, aby sa predišlo neúmyselnej expozícii citlivých zdrojov.

https://cybersecuritynews.com/azure-private-endpoint-exposes-azure-resources/

---

### Microsoft Teams pripravuje automatické zdieľanie pracovnej polohy cez Wi-Fi

Microsoft pracuje na novej funkcii pre Teams, ktorá bude automaticky detegovať a zobraziť fyzickú pracovnú polohu používateľa na základe jeho pripojenia k firemnému Wi-Fi a zdieľať ju v rámci organizácie, pričom sa má spustiť v marci 2026. Funkcia je navrhnutá pre desktopové verzie na Windows a macOS a je vypnutá v predvolenom nastavení, pričom ju musia povoliť tenant administrátori a používatelia si musia opt-in. Systém používa identifikátory Wi-Fi sietí (SSID) na mapovanie na konkrétne budovy, čím umožňuje automaticky aktualizovať „Work Location“ status a odstraňuje potrebu manuálnych aktualizácií. Microsoft obhajuje zmenu ako pomoc pre hybridné tímy pri koordinácii prítomnosti, no kritici upozorňujú na potenciálne obavy o súkromie a sledovanie zamestnancov, aj keď je aktualizácia limitovaná na pracovnú dobu a vyžaduje súhlas používateľa.

https://cybersecuritynews.com/microsoft-teams-share-your-location/

---

### Cloud malware VoidLink vykazuje jasné známky AI generácie

Bezpečnostní výskumníci odhalili nový cloudový malvér s názvom VoidLink, pri ktorom analýza naznačuje, že bol vo veľkej miere vytvorený pomocou generatívnej umelej inteligencie. Kód obsahuje opakujúce sa vzory, zvláštne štruktúry a neefektívne obfuskácie typické pre automaticky generované programy, čo naznačuje minimálny manuálny zásah útočníkov. VoidLink je navrhnutý na kompromitovanie cloudových prostredí, kde sa snaží získať perzistentný prístup, mapovať infraštruktúru a sťahovať ďalšie škodlivé moduly. Prípad poukazuje na rastúci trend zneužívania AI na rýchlu tvorbu malvéru, čo mení spôsob, akým útočníci vyvíjajú a nasadzujú škodlivé nástroje.

https://www.bleepingcomputer.com/news/security/voidlink-cloud-malware-shows-clear-signs-of-being-ai-generated/