Cybersecurity Report

6.4.2026 – 19.4.2026

Nárast e-mailových červov prináša novú vlnu hrozieb pre priemyselné siete

Bezpečnostní analytici upozorňujú na výrazný rast email-borne worm kampaní, ktoré sa šíria cez phishingové správy a zasahujú aj priemyselné a firemné siete. Hlavným aktérom je variant XWorm, ktorý po otvorení škodlivej prílohy umožňuje vzdialené ovládanie zariadenia, krádež dát a ďalšie šírenie v sieti. Útočníci využívajú sociálne inžinierstvo, pričom prílohy maskujú ako životopisy, faktúry alebo interné dokumenty. Trend ukazuje, že tradičný e-mail phishing ostáva efektívnym vektorom aj proti kritickej infraštruktúre a OT prostrediam.

https://cybersecuritynews.com/email-borne-worm-surge-drives-new-threat/

108 škodlivých Chrome rozšírení kradlo dáta a zneužívalo prehliadače používateľov

Bezpečnostní výskumníci odhalili koordinovanú kampaň zahŕňajúcu 108 škodlivých Chrome rozšírení, ktoré boli dostupné v oficiálnom Chrome Web Store a spolu zasiahli približne 20 000 používateľov. Rozšírenia sa tvárili ako legitímne nástroje, no v pozadí kradli údaje z Google účtov, unášali Telegram relácie, vkladali reklamy a spúšťali vlastný JavaScript na navštívených stránkach. Všetky komunikovali s rovnakou C2 infraštruktúrou, čo naznačuje centralizovanú operáciu. Incident opäť potvrdzuje, že browser extensions predstavujú významný útokový vektor a organizácie by mali pravidelne auditovať povolené doplnky a ich oprávnenia.

https://thehackernews.com/2026/04/108-malicious-chrome-extensions-steal.html

Windows Defender 0-day chyba je aktívne zneužívaná útočníkmi

Bezpečnostní výskumníci upozornili na novú 0-day zraniteľnosť vo Windows Defender, ktorá je už aktívne zneužívaná v útokoch. Chyba umožňuje útočníkom po získaní lokálneho prístupu eskalovať oprávnenia, vypnúť ochranné mechanizmy alebo získať vyšší prístup k systému, čím sa výrazne uľahčuje nasadenie ďalšieho malvéru. Incident ukazuje, že aj natívne bezpečnostné riešenia môžu predstavovať atraktívny cieľ pre útočníkov pri post-exploitation aktivitách. Organizáciám sa odporúča okamžite aplikovať dostupné aktualizácie, monitorovať neštandardné zmeny v Defender konfigurácii a posilniť detekciu privilege escalation techník.

https://cybersecuritynews.com/windows-defender-0-day-vulnerability-exploited/

KCKB UPJS | Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | CSIRT UPJS

Ukradnuté prihlasovacie údaje robia z MFA ďalší cieľ útoku

Bezpečnostní analytici upozorňujú, že pri kompromitovaných účtoch už samotné MFA nemusí stačiť, keďže útočníci čoraz častejšie využívajú phishing relay (AiTM), krádež session tokenov, MFA fatigue kampane alebo sociálne inžinierstvo voči helpdesku. V takýchto scenároch útočník neobchádza autentifikáciu technicky, ale zneužíva legitímny prihlasovací proces a ľudský faktor. Tradičné metódy ako SMS kódy, push notifikácie či TOTP tak nemusia zabrániť prevzatiu účtu pri dobre pripravenej kampani. Odborníci preto odporúčajú phishing-resistant autentifikáciu, FIDO2/WebAuthn, biometrické overenie a silnejšiu ochranu identity počas celého login procesu.

https://www.bleepingcomputer.com/news/security/when-attackers-already-have-the-keys-mfa-is-just-another-door-to-open/

Google Chrome zavádza ochranu proti krádeži session cookies infostealer malvérom

Google nasadil v Chrome 146 pre Windows novú bezpečnostnú funkciu Device Bound Session Credentials (DBSC), ktorá má zabrániť zneužitiu ukradnutých session cookies pri prevzatí účtov. Mechanizmus kryptograficky viaže reláciu používateľa na konkrétne zariadenie pomocou hardvérovej ochrany, napríklad TPM čipu, takže odcudzené cookies nemožno použiť na inom systéme. Ide o reakciu na rastúce kampane infostealer malvéru, ktoré kradnú autentifikačné tokeny a obchádzajú MFA bez znalosti hesla. Google uvádza, že pri skorom testovaní DBSC zaznamenal výrazný pokles úspešných session hijacking útokov.

https://www.bleepingcomputer.com/news/security/google-chrome-adds-infostealer-protection-against-session-cookie-theft/