UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Centrum informačných a komunikačných technológií

Úsek informačnej a kybernetickej bezpečnosti
Tím na riešenie počítačových bezpečnostných incidentov (CSIRT-UPJS)
Šrobárova 2, 041 80 Košice
VoIP: +421 (055) 234 2425, IČO: 00397768
csirt@upjs.sk, https://csirt.upjs.sk/

TLP:CLEAR

Týždenná správa csirt.upjs.sk
7.1.2025 – 9.1.2025

TLP:CLEAR

Vypracoval: csirt.upjs.sk

Zanedbané domény zneužívané v malspamových kampaniach na obchádzanie bezpečnostných opatrení

Útočníci zneužívajú zanedbané, nepoužívané domény, ktoré často postrádajú správne DNS záznamy, na obchádzanie bezpečnostných mechanizmov SPF a DMARC. Tieto domény im umožňujú falšovať odosielateľské adresy a obísť ochranné opatrenia, čo vedie k úspešnému doručeniu malspamových kampaní.

Top 5 malvérových hrozieb, na ktoré sa treba pripraviť v roku 2025

Rok 2024 priniesol množstvo vysokoprofilových kybernetických útokov a tento trend bude pokračovať aj v roku 2025. Článok predstavuje 5 bežných rodín malvéru. Zahŕňajú Lumma, ktorý kradne citlivé údaje, XWorm umožňujúci vzdialený prístup útočníkom, NKAbuse využívajúci blockchain technológie, Triangulation zameraný na špionáž cez iOS zariadenia a CloudSorcerer/EastWind, ktorý exfiltruje dáta cez verejný cloud.

Banshee 2.0: Malvér zneužívajúci Apple šifrovanie na macOS

Banshee, malvér šírený ako „stealer-as-a-service," kradne prihlasovacie údaje a kryptomenové peňaženky. Vylepšená verzia z roku 2024 využíva šifrovací algoritmus z Apple XProtect, čím efektívne obchádza detekciu antivírusovými programami. Táto technika spôsobila, že až 65 antivírusových enginov nedokázalo identifikovať jeho prítomnosť.

CISA varuje pred kritickými zraniteľnosťami v Oracle WebLogic Server a Mitel MiCollab

Zraniteľnosť CVE-2024-41713 v komponente NuPoint Unified Messaging (NPM) platformy Mitel MiCollab umožňuje útočníkom vykonávať neoprávnené administratívne akcie a získať prístup k informáciám o používateľoch a sieti. Zraniteľnosť CVE-2020-2883 v Oracle WebLogic Server, opravená v apríli 2020, umožňuje neautentifikovaným útočníkom vzdialene prevziať kontrolu nad neaktualizovanými servermi. CISA odporúča okamžité aktualizácie systémov na ochranu pred týmito hrozbami.

Gravy Analytics Hack odhaľuje skryté zhromažďovanie údajov o polohe prostredníctvom obľúbených aplikácií

Nedávny útok na spoločnosť Gravy Analytics v oblasti údajov o polohe odhalil, ako boli tisíce populárnych aplikácií vrátane Candy Crush, Tinder a MyFitnessPal zneužité na zhromažďovanie údajov o polohe používateľov bez ich vedomia. K tomuto zhromažďovaniu údajov dochádza prostredníctvom reklamného ekosystému prostredníctvom procesov ponúkania cien v reálnom čase (RTB), a nie prostredníctvom kódu vloženého samotnými vývojármi aplikácií. Uniknuté údaje zahŕňajú desiatky miliónov súradníc mobilných telefónov zo zariadení v USA, Rusku a Európe, ktoré sú prepojené s rôznymi aplikáciami od hier a zoznamovacích platforiem až po náboženské a zdravotné aplikácie.