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 20.1.2025 – 26.1.2025

TLP:CLEAR

Vypracoval: csirt.upjs.sk

Trump ukončil členstvo v poradnom výbore DHS, čím narušil kontrolu kybernetickej bezpečnosti

Trumpova administratíva ukončila členstvo vo všetkých poradných výboroch Ministerstva vnútornej bezpečnosti (DHS), vrátane výborov zameraných na kybernetickú bezpečnosť, umelú inteligenciu a infraštruktúru. Medzi zrušenými výbormi je aj Cyber Safety Review Board, ktorý v minulosti kritizoval Microsoft za zlyhania vedúce k útokom čínskej hackerskej skupiny. Tento krok vyvolal obavy z oslabenia národnej bezpečnosti, pričom kritici, ako senátor Ron Wyden, označili rozhodnutie za dar čínskym špiónom. Rozhodnutie zároveň vyvoláva podozrenia z možnej politickej odplaty voči Microsoftu.

Stovky falošných stránok Reddit obsahujú malvér Lumma Stealer

Hackeri vytvorili takmer 1 000 falošných webových stránok napodobňujúcich Reddit a WeTransfer, aby šírili malvér Lumma Stealer. Na týchto falošných stránkach sa zobrazuje nepravá diskusia, kde jeden používateľ žiada o pomoc pri stiahnutí nástroja, iný poskytuje odkaz na údajný súbor na WeTransfer, a tretí ďakuje za pomoc, čím celá konverzácia pôsobí dôveryhodne. Tieto falošné stránky obsahujú názvy napodobňovaných značiek s náhodnými číslami a znakmi, aby na prvý pohľad vyzerali legitímne, a používajú domény ".org" alebo ".net". Výskumník Sekoia identifikoval 529 stránok napodobňujúcich Reddit a 407 stránok napodobňujúcich WeTransfer.

Nezabezpečené protokoly tunelovania odhaľujú 4,2 milióna hostiteľov vrátane sietí VPN a smerovačov

Výskum odhalil zraniteľnosti v tunelovacích protokoloch, ako sú IP6IP6, GRE6, 4in6 a 6in4, ktoré bez autentifikácie a šifrovania umožňujú útočníkom vykonávať rôzne útoky. Až 4,2 milióna zariadení, vrátane VPN serverov, domácich routerov a jadrových internetových routerov, je týmto ohrozených. Útočníci môžu tieto zraniteľnosti zneužiť na anonymné útoky, prístup do súkromných sietí a vykonávanie DDoS útokov. Odporúča sa implementovať bezpečnostné opatrenia, ako je použitie protokolov IPSec alebo WireGuard na autentifikáciu a šifrovanie, a prijímať tunelovacie pakety len z dôveryhodných zdrojov.

Rekordný DDoS útok dosiahol 5,6 Tbps

Spoločnosť Cloudflare zaznamenala v roku 2024 nárast frekvencie DDoS útokov o 53 %, pričom zablokovala približne 21,3 milióna útokov. Najvýznamnejší z nich bol útok s intenzitou 5,6 terabitov za sekundu (Tbps), ktorý trval 80 sekúnd a pochádzal z botnetu odvodeného od Mirai, zahŕňajúceho 13 000 unikátnych IP adries. Tento útok bol zameraný na poskytovateľa internetových služieb vo východnej Ázii. Predchádzajúci rekordný útok mal intenzitu 3,8 Tbps. Medzi najčastejšie vektory útokov na sieťovej vrstve patrili SYN flood (38 %), DNS flood (16 %) a UDP flood (14 %). V štvrtom štvrťroku 2024 pochádzalo 73 % HTTP DDoS útokov od známych botnetov, pričom 92 % týchto útokov bolo realizovaných cez HTTPS.

Útok na dodávateľský reťazec cielil na Chrome rozšírenia

V decembri 2024 hackeri kompromitovali minimálne 35 rozšírení prehliadača Google Chrome, čím ohrozili viac ako 2,6 milióna používateľov. Útok začal phishingom na vývojárov, od ktorých útočníci získali prístup cez OAuth a následne nahrali škodlivé verzie rozšírení. Malvér kradol citlivé údaje, vrátane API kľúčov, cookies a tokenov, pričom sa zameriaval na používateľov Facebook Business a OpenAI ChatGPT.