TLP:CLEAR

Prehľad bezpečnostných udalostí csirt.upjs.sk 27.1.2025 – 07.2.2025

DeepSeek čelí koordinovaným DDoS útokom

Spoločnosť DeepSeek, známa svojimi pokrokmi v oblasti umelej inteligencie, sa od 20. januára 2025 stala terčom rozsiahlych DDoS útokov. Útoky sa zamerali na API rozhranie a chatovací systém, pričom útočníci využívali techniky odrazu prostredníctvom protokolov NTP a memcached. Po zmene IP adresy 28. januára útočníci rýchlo prispôsobili svoje metódy a pokračovali v útokoch na hlavné domény spoločnosti. Infraštruktúra útokov bola prevažne umiestnená v USA (20 %), Spojenom kráľovstve (17 %) a Austrálii (9 %).

Microsoft opravuje kritické zraniteľnosti v Azure AI Face Service a Microsoft Account

Microsoft vydal aktualizácie na odstránenie dvoch kritických bezpečnostných chýb. Zraniteľnosť **CVE-2025-21396** (CVSS 7,5) umožňovala eskaláciu privilégií v službe Microsoft Account v dôsledku chýbajúcej autorizácie, čo mohlo útočníkovi umožniť získať vyššie oprávnenia. Druhá zraniteľnosť, **CVE-2025-21415** (CVSS 9,9), sa týkala služby Azure AI Face Service a umožňovala obísť autentifikáciu pomocou spoofingu a následne eskalovať privilégiá v sieti. Microsoft uviedol, že obe zraniteľnosti boli úplne mitigované a zákazníci nemusia podniknúť žiadne ďalšie kroky.

Pokles platieb za ransomware o 35 % v roku 2024

V roku 2024 došlo k výraznému poklesu platieb za ransomware o 35 %, pričom celková suma dosiahla 813,55 milióna dolárov, čo je pokles z 1,25 miliardy dolárov v roku 2023. Iba približne 30 % obetí, ktoré vstúpili do rokovaní s útočníkmi, nakoniec zaplatilo výkupné. Tento pokles je pripisovaný zvýšenej odolnosti obetí voči plateniu výkupného, zlepšenej informovanosti o rizikách spojených s ransomware útokmi a intenzívnejším zásahom orgánov činných v trestnom konaní proti ransomvérovým skupinám. Napriek tomu bol rok 2024 poznačený rekordným výkupným vo výške 75 miliónov dolárov zaplateným skupine Dark Angels a celkovým počtom 5 263 úspešných ransomvérových útokov.

Zneužitie popularity DeepSeek na šírenie škodlivých balíkov cez PyPI

Dňa 29. januára 2025 boli na repozitári **Python Package Index (PyPI)** zverejnené dva škodlivé balíky s názvami **deepseeek** a **deepseekai**, ktoré sa vydávali za klientské knižnice pre prácu s **DeepSeek AI API**. Tieto balíky obsahovali funkcie na zber údajov o používateľoch, počítačoch a environmentálnych premenných, vrátane API kľúčov a prihlasovacích údajov. Údaje boli odosielané na server riadený cez platformu **Pipedream**. Balíky boli stiahnuté 36-krát predtým, než ich administrátori PyPI odstránili. Incident poukazuje na rastúce využívanie AI nástrojov útočníkmi pri tvorbe škodlivého kódu a na potrebu opatrnosti pri používaní nových balíkov, ktoré sa prezentujú ako rozhrania pre populárne služby.

Nárast zneužitých zraniteľností v roku 2024

V roku 2024 bolo aktívne zneužitých **768 CVE zraniteľností**, čo je 20 % nárast oproti roku 2023. Až **23,6 %** z nich bolo využitých v deň zverejnenia alebo skôr. Medzi najčastejšie zneužívané patrí **CVE-2021-44228** (Log4j), pričom celkovo zostáva **400 000 systémov** zraniteľných voči bezpečnostným chybám v produktoch od **Microsoft, Cisco, Fortinet, Citrix a ďalších**.