TLP:CLEAR

Prehľad bezpečnostných udalostí csirt.upjs.sk 17.3.2025 – 21.3.2025

SANS Institute varuje pred novými cloudovými útokmi zneužívajúcimi API

Výskumníci zo SANS Institute upozorňujú na novú vlnu kybernetických útokov, ktoré cielia na cloudové služby prostredníctvom zneužitia API rozhraní. Útočníci využívajú nesprávne nakonfigurované oprávnenia a nedostatočne zabezpečené autentifikačné mechanizmy na získanie neoprávneného prístupu k citlivým údajom. Podľa zistení ide o sofistikované techniky, ktoré zahŕňajú manipuláciu s API požiadavkami a obchádzanie bezpečnostných kontrol bez potreby tradičných phishingových útokov. Výskumníci zaznamenali zvýšený počet incidentov zameraných na poskytovateľov cloudových riešení, pričom útočníci sa snažia maskovať svoju aktivitu legitímne vyzerajúcimi požiadavkami na služby.

Zraniteľnosť v ChatGPT ohrozuje organizácie, útočníci ju aktívne zneužívajú

Bezpečnostní experti odhalili zraniteľnosť v ChatGPT, ktorú útočníci aktívne zneužívajú na získanie neoprávneného prístupu k citlivým údajom organizácií. Chyba sa týka nesprávneho spracovania API požiadaviek, čo umožňuje útočníkom manipulovať s reláciami a extrahovať dáta z konverzácií. Výskumníci zaznamenali prípady, keď útočníci využívali túto metódu na prístup k interným firemným informáciám či zdrojovým kódom. Hoci OpenAI už vydala opravu, nie je jasné, do akej miery boli organizácie kompromitované.

Útok na GitHub Actions pravdepodobne spustil reťazový supply chain útok

Výskumníci identifikovali sofistikovaný útok na GitHub Actions, ktorý mohol viesť k ďalšiemu reťazovému supply chain útoku. Útočníci zneužili nesprávne nakonfigurované pracovné postupy v GitHub Actions na získanie neoprávneného prístupu k vývojárskym prostrediam. Následne mohli manipulovať s legitímnymi softvérovými balíkmi a šíriť škodlivý kód medzi závislosťami v open-source ekosystéme. Tento incident naznačuje, že útočníci sa stále častejšie zameriavajú na automatizované nástroje CI/CD na kompromitovanie dodávateľských reťazcov softvéru.

Operácia FishMedley: Nová kyberšpionážna kampaň zameraná na diplomaciu a výskum

Výskumníci z ESET odhalili kyberšpionážnu operáciu FishMedley, ktorá cieli na diplomatické a výskumné inštitúcie. Útočníci využívajú sofistikované metódy infikovania systémov, pričom sa zameriavajú na kompromitáciu e-mailových účtov a distribuovanie škodlivého kódu cez phishingové kampane. Malvér použitý v útoku umožňuje vzdialené ovládanie napadnutých zariadení, kradnutie citlivých údajov a monitorovanie aktivít obetí. Analýza naznačuje, že za útokmi môže stáť štátom sponzorovaná skupina, keďže techniky a ciele sú v súlade s dlhodobými spravodajskými operáciami.

Medusa ransomware využíva škodlivý ovládač AbyssWorker na obchádzanie zabezpečenia

Výskumníci odhalili, že Medusa ransomware používa nový škodlivý ovládač nazývaný AbyssWorker na vypnutie bezpečnostných riešení pred šifrovaním súborov. Tento ovládač umožňuje útočníkom deaktivovať antivírusové programy a ochranné mechanizmy Windows, čím zvyšuje účinnosť útoku. Medusa ransomware sa šíri prostredníctvom phishingových e-mailov a exploitov, pričom po infikovaní systému zašifruje dáta a požaduje výkupné.