Forenzički izveštaj [FR225UK579]

Nadležni forenzičar: John Doe
Uzorak podnesen od strane: JiSecBlue
Adresa entiteta koji je podneo uzorak: Trg slobode 1, Novi Sad

Naziv pretnje: CryptoLeech
Opis ponašanja: Zlonamerni paket kompromituje CI/CD procese i ubacuje skriveni kod.
Nivo pretnje: Srednji
Heš uzorka: cd4bf915417f465cb1fee9417924de4d

Sažetak

CryptoLeech je malver usmeren na npm ekosistem koji kompromituje pakete kroz lanac zavisnosti. Nakon infekcije, krade tokene i omogućava daljinski pristup napadaču. Preporučuje se hitna rotacija kredencijala i detaljna analiza svih zahvaćenih repozitorijuma.