

Forenzički izveštaj [FR613UK932]

Nadležni forenzičar: John Doe

Uzorak podnesen od strane: JiSecBlue

Adresa entiteta koji je podneo uzorak: Trg slobode 1, Novi Sad

Naziv pretnje: ShadowInjector

Opis ponašanja: Samoreplicirajući npm crv koji kompromituje pakete i eksfiltrira tokene.

Nivo pretnje: Srednji

Heš uzorka: 69237f2f53fdd1eb300f0dec670c4470

Sažetak

ShadowInjector 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.