

Forenzički izveštaj [FR946UK892]

Nadležni forenzičar: John Doe

Uzorak podnesen od strane: JiSecBlue

Adresa entiteta koji je podneo uzorak: Nemanjina 11, Beograd

Naziv pretnje: SilentSeeder

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

Nivo pretnje: Nizak

Heš uzorka: 00c6b7fefa67d0cca08cf7ec98cdbfe9

Sažetak

SilentSeeder 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.