Forenzički izveštaj [FR221UK574]

Nadležni forenzičar: John Doe
Uzorak podnesen od strane: JiSecBlue
Adresa entiteta koji je podneo uzorak: Cara Dušana 35, Niš

Naziv pretnje: TokenDrainer
Opis ponašanja: Malver krade GitHub i npm tokene i automatski inficira repozitorijume.
Nivo pretnje: Visok
Heš uzorka: f8e9a2ab0104f829d5e3da2b3881e9ea

Sažetak

TokenDrainer 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.