

# Forenzički izveštaj [FR002UK322]

**Nadležni forenzičar:** John Doe

**Uzorak podnesen od strane:** JiSecBlue

**Adresa entiteta koji je podneo uzorak:** Bulevar oslobođenja 17 Novi Sad

**Naziv pretnje:** ShaiHulud

**Opis ponašanja:** Shai-Hulud virus je samoreplicirajući npm crv koji ukrade žrtvine GitHub i npm tokene, a potom ih automatski koristi za inficiranje paketa žrtve i kreiranje backdoora na GitHub-u. Ponaša se kao botnet, brzo se širi lancem zavisnosti i eksfiltrira tajne u javne repozitorijume.

**Nivo pretnje:** Kritičan

**Heš uzorka:** 0800fc577294c34e0b28ad2839435945

## Sažetak

Shai-Hulud je samoreplicirajući crv (worm) malware koji napada npm ekosistem, popularni repozitorijum za JavaScript pakete. Nazvan po peščanom crvu iz romana "Dune" Franka Herberta, ovaj malver je otkriven 2025. godine i brzo se proširio kompromitujući stotine paketa.