

Naziv Zaposlenog: Nikola Milić

Bezbednosna Organizacija: Centar za Cyber Bezbednost Kragujevac

Pogodjena Organizacija: Univerzitet u Kragujevcu

Ozbiljnost Incidenta: visoka

Adresa Pogodjene Organizacije: Svetozara Markovića 69, Kragujevac

Opis incidenta:

Tokom redovne sigurnosne provere Univerziteta u Kragujevcu, otkriven je napad putem zlonamernog softvera koji je uspeo da zaobiđe antivirusnu zaštitu i inficira radne stanice određenog broja profesora i administrativnog osoblja. Radi se o sofisticiranom trojancu koji omogućava daljinski pristup napadačima i krađu poverljivih akademskih podataka.

Pošto su incident detektovali stručnjaci centra, izvršena je hitna izolacija pogođenih računara i kompletno čišćenje mreže. Paralelno je sprovedena istraga o poreklu malvera, a sigurnosni tim je obavestio sve zaposlene i studente o rizicima i merama koje treba da preduzmu.

U svetlu ovog incidenta, Univerzitet je uveo strože sigurnosne protokole, uključujući automatizovane skenere za malver, obaveznu edukaciju zaposlenih o sajber pretnjama i primenu naprednih metoda zaštite kao što su endpoint detection & response (EDR).