Dev gets 4 years for creating kill switch on ex-employer&#039;s systems

Data: 2025-08-21 23:46:55

Autor: Inteligência Against Invaders

A software developer has been sentenced to four years in prison for sabotaging his ex-employer’s Windows network with custom malware and a kill switch that locked out employees when his account was disabled.

Davis Lu, 55, a Chinese national living legally in Houston, worked for an Ohio-based company, reportedly Eaton Corporation, from 2007 until his termination in 2019.

After acorporate restructuring and subsequentdemotion in 2018, the DOJ says that Lu retaliated by embedding malicious code throughout the company’s Windows production environment.

The malicious code included an infinite Java thread loop designed to overwhelm servers and crash production systems.

Lu also created a kill switchnamed “IsDLEnabledinAD” (“Is Davis Lu enabled in Active Directory”)that would automatically lock all users out of their accounts if his account was disabled in Active Directory.

When his employment was terminated on September 9, 2019, and his account disabled, the kill switch activated, causing thousands of users to be locked out of their systems.

“The defendant breached his employer’s trust by using his access and technical knowledge to sabotage company networks, wreaking havoc and causing hundreds of thousands of dollars in losses for a U.S. company,” said Acting Assistant Attorney General Matthew R. Galeotti.

When he was instructed to return his laptop, Lu reportedly deleted encrypted data from his device. Investigators later discovered search queries on the device researching how to elevate privileges, hide processes, and quickly delete files.

Lu was found guilty earlier this year of intentionally causing damage to protected computers. After his four-year sentence, Lu will also serve three years of supervised release following his prison term.

[IMAGEM REMOVIDA]