When the Insider Becomes the Threat

Infosources™

August 23, 2025

Cybersecurity defenses are often built to keep attackers out — but sometimes the real danger comes from the inside. Employees with legitimate access and technical knowledge can inflict severe damage if they choose to turn against their organization. Insider threats are among the hardest risks to mitigate because they bypass many of the traditional safeguards that protect networks from external hackers. The case of a former Eaton developer illustrates how one individual's decision to weaponize his access brought down critical systems, caused financial losses, and ultimately landed him in prison.

The case of Davis Lu illustrates in a striking way how insider threats unfold when technical access, organizational changes, and personal resentment collide. Lu, a 55-year-old, Chinese national, software developer, had been with his employer since 2007, working within the IT backbone of Eaton Corporation, a major U.S. power management company. Things changed in 2018 during a corporate realignment, when his responsibilities and access were scaled back. What looked on the surface like a normal restructuring planted the seeds for an act of sabotage that would later cripple the company's systems.

By mid-2019, Lu had begun inserting malicious code into Eaton's infrastructure. He embedded infinite loops in source code to crash servers by endlessly spawning new Java threads. He deleted profile files that his colleagues needed to log in. And he went further, preparing what he called a kill switch: a piece of code that automatically locked out every user if his own Active Directory credentials were disabled. He even gave it a personal marker — naming it *IsDLEnabledinAD* — shorthand for "Is Davis Lu enabled in Active Directory." It was pre-wired to activate the moment the company tried to cut him off.

That moment came on September 9, 2019, when Lu was placed on leave and asked to return his company laptop. As soon as his account was disabled, the kill switch fired. Thousands of users around the world were suddenly locked out of their systems. Eaton's operations were disrupted on a global scale, costing the company hundreds of thousands of dollars.

The sabotage was not just technical but psychological. Lu left behind code labeled *Hakai* ("destruction" in Japanese) and *HunShui* ("sleep" in Chinese), signaling intent and perhaps even a twisted sense of authorship. On his final day with the laptop, he went further still — deleting encrypted volumes, attempting to wipe Linux directories, and erasing other projects. His internet history revealed searches on privilege escalation, hiding processes, and file deletion — showing clear premeditation and efforts to obscure what he had done.

The Department of Justice later described his actions as a deliberate abuse of trust, a calculated effort to use insider access to wreak havoc on a U.S. company. For this, Lu was arrested in 2021, convicted in 2025, and sentenced to four years in prison with an additional three years of supervised release.

The case underlines the persistent risk of insider threats: trusted employees who understand the systems more deeply than any outsider ever could. Here, the warning signs were visible in hindsight — reduced responsibilities, technical expertise, resentment, and lingering access. Once the trigger was pulled, the impact was immediate and devastating. For investigators and companies alike, the lesson is clear: technical defenses mean little if the enemy is already inside the gates.