# German nuclear plant’s fuel rod system swarming with old malware

By Sean Gallagher

Published: 2016-04-27 · Archived: 2026-04-06 01:00:31 UTC

A nuclear power plant 75 miles from Munich has been harboring malware—including remote-access trojans and file-stealing malware—on the computer system that is used to monitor the plant’s fuel rods. Fortunately, as Reuters reported, the computer isn’t connected to the Internet, and the malware was never able to be activated.

The malware was discovered on computer systems at the Gundremmingen nuclear power facility by employees of the German electrical utility company RWE. It included Conficker, a worm first detected in 2008 designed to steal user credentials and personal financial data and turn infected computers into “bots” to carry out distributed denial of service (DDoS) attacks. W32.Ramnit, a worm that provides attackers with a remote access tool and allows them to steal files and inject code into webpages to capture banking data, was also discovered on the system.

In addition to the infected computer system, last upgraded in 2008, malware was discovered on 18 USB removable storage devices. Both Conficker and W32.Ramnit spread themselves through USB drives. The malware did no harm because it required Internet access to contact a command-and-control network, and it appears that the plant was not specifically targeted by attackers since the malware was focused largely on financial fraud.

---