# Malware Shuts Down German Nuclear Power Plant on Chernobyl's 30th Anniversary

By Catalin Cimpanu

Published: 2016-04-26 · Archived: 2026-04-05 15:37:29 UTC

**A routine security audit has discovered malware on the computer systems of the Gundremmingen nuclear power plant in Germany. RWE, the plant's operator, shut down the power plant for precaution, despite saying it was nothing serious.**

According to a press release put out by Gundremmingen power plant officials, the malware was discovered on the plant's Block B IT network that handles the fuel handling system.

## The malware infection was most likely an accident, not an attack

The malware affected only the computer IT systems and not the ICS/SCADA equipment that interacts with the nuclear fuel. Officials say the equipment's role is to load and unload nuclear fuel from the power plant's Block B and then transfer old fuel to the storage pool.

Gundremmingen officials said the IT system was not connected to the Internet and that they suspect someone brought in the malware by accident on a USB thumb drive, either from home or computers found in the power plant's facility.

Authorities did not reveal the name of the malware strain but said it was nothing serious, classifying the whole incident as "N" (normal category).

## Today is Chernobyl disaster's 30$^{th}$ anniversary

The malware infection was discovered Sunday on April 24, and two days later the power plant is still offline. Today, April 26, 2016, marks 30 years since the Chernobyl nuclear power plant disaster.

The nuclear plant is now going through all the security procedures involved with such events, with its staff scanning all other computer systems and going through all the regular checks and motions before putting the plant back into production.

The Gundremmingen nuclear power plant is considered one of Germany's most outdated nuclear power plants. Gundremmingen is set to permanently shut down in 2021, but over 750 people protested over the weekend in the hope of convincing authorities to shut down the two reactors left working before the final deadline.

“Eugene Kaspersky: It’s not surprising”

Eugene Kaspersky, founder and CEO of Kaspersky Lab, one of the world's leading security firms, put the situation in perspective for *Softpedia*.

"An industrial control system used for loading nuclear fuel elements at Germany's Gundremmingen nuclear power plant has been infected with malware. Yes, alarm bells are probably ringing in everyone's head who's just read that. Thing is, it's not surprising. What is rather surprising is that we don't hear such worrying news more frequently."

"From what we know, it was not a targeted attack on the power plant's system; it was just a 'regular' infection, contracted most likely by someone connecting a storage device to the system. That's what we hear from German media."

"What it shows is the main, basic issue of today's connected systems: critical infrastructure is as vulnerable as all other systems connected to the Internet. We saw the example of the blast furnace being destroyed by a malware attack (disclosed by Germany's Federal Office for Information Security); there was Stuxnet – malware allegedly designed to physically destroy nuclear enrichment facilities in Iran."

"Operators and regulators have to understand that in an age when we see more than 310,000 new samples of malware a day, some of those samples might damage systems they were never intended to be aimed at. For such cases – of course in addition to intentional direct attacks – we have to be prepared."

Only a week ago, Kaspersky became the first big antivirus company to provide a **cyber-security solution for ICS/SCADA equipment**.

**UPDATE:** According to reports in the Germany media, the malware found inside the nuclear plant were versions fo the Ramnit banking trojan and the Conficker worm.

---

Source: https://news.softpedia.com/news/on-chernobyl-s-30th-anniversary-malware-shuts-down-german-nuclear-power-plant-503429.shtml