Multiple Computer Viruses Have Been Discovered in This German Nuclear Plant

By Peter Dockrill

Published: 2016-04-28 · Archived: 2026-04-05 14:34:02 UTC

Markus Gann/Shutterstock.com

The potential dangers of USB sticks when it comes to transporting computer viruses are well known, but even workers in highly sensitive environments like nuclear facilities can't always seem to prevent themselves from exposing their PCs to malware.

The operators of the Gundremmingen nuclear power plant in Germany announced this week that the station has been infected with numerous computer viruses during a routine inspection on the weekend.

Malware was detected on a computer installed with data visualisation software used in conjunction with the plant's fuel assembly loading machine. Viruses were also found on 18 removable drives in use in the facility, such as USB keys and external hard drives.

But the company maintains that there is no risk to the public or staff, as the operating software running on the infected system doesn't give it any actual controls over the fuel assembly loader, and the system is cut off from the internet – meaning that any viruses infecting the computer can't report back to base or attempt to download any additional malware.

The plant's representatives said all sensitive areas in the facility are isolated from the web to help protect against any kind of malware manipulation, and that IT staff had terminated the viruses after finding them in a check on Sunday. The company says it's stepping up security after the incident.

Among the viruses detected were "W32.Ramnit" and "Conficker" - two worms that target Microsoft Windows systems. W32.Ramnit was first discovered on PCs in 2010, and is spread through removable drives, designed to enable remote attackers to access compromised PCs. Conficker is a more versatile threat that can propagate

through networks, and is estimated by security software firm Symantec to have infected upwards of 3 million computers.

While both these viruses are considered relatively low-risk malware – and the incident at Gundremmingen has itself been graded as the least dangerous level on the International Nuclear Event Scale – it's nonetheless a disturbing occurrence. And it serves as a reminder of how easily even locked-down, critical infrastructure like nuclear power plants – where security is of the upmost importance – can't seem to keep technological threats out entirely.

Mikko Hypponen, chief research officer for Finland's F-Secure, told Christoph Steitz and Eric Auchard at Reuters that these kinds of breaches were surprisingly common, where general malware finds its way into systems in specialised environments.

But Hypponen says the risk is generally low unless critical infrastructure has been specifically targeted, as the malware that targets popular systems like Windows and Android hasn't been designed to find its way around systems used in nuclear power plants and plane cockpits, for example, so poses little threat.

That said, the fact that workers are clearly still unintentionally compromising their own systems with malware on removable drives is something we need to be aware of. Germany's Federal Office for Information Security warned of the likelihood of such an event in a report issued just last year, and until staff in places like nuclear power plants take these warnings more seriously, more breaches like this will occur.

We can only hope the next incident is as consequence-free as it was this time around…
