Malware Discovered in German Nuclear Power Plant

Archived: 2026-04-05 17:36:11 UTC

A German nuclear power plant was recently discovered to be infested by computer malware, reports say on Tuesday. The Gundremmingen plant, operated by the German utility RWE and nestled northwest of Munich, is said to have the highest-output nuclear power station in Germany. Experts identified the viruses to be “W32.Ramnit” and “Conficker”, found at the plant’s B unit in the system that involves the transport of reactor fuel. However, as it appears, the discovered malware are unlikely to threaten the operations of the plant, which has systems that are isolated from the internet.

Experts are looking into the possibility of a malware-infested USB unknowingly used by an employee as the point of entry of the malware into the nuclear power plant’s system. Recent reports found that malware was seen in 18 removable drives, commonly on USB sticks used and “maintained separately from the plant’s operating systems”.

While investigations done by Germany’s Federal Office for Information Security (BSI) and a pool of security analysts are currently ongoing, this prompted a heightened cyber-security alert. In a statement, Tobias Schmidt, spokesman for the Gundremmingen nuclear plant noted, “*Systems that control the nuclear process are analog, thus isolated from cyber threats. These systems are designed with security features that protect them against manipulation.*”

According to initial investigations, the discovered viruses were not created to target power plants but were simply common malware variants. W32.Ramnit, which is said to target Microsoft Windows software, commonly spreads through data sticks. Upon infection, this malware gives an attacker remote access of connected systems. Aside from this, the malware has the capability to steal data from its infected systems. Similarly, Conficker, first sighted in back in 2008, is distributed across networks by dropping copies of itself in removable drives and network shares.

Interestingly, this news follows the release of a studynews article indicating the vulnerability of German nuclear power plants to terror-attacks. While the discovery of the said malware is different from the previously reported incidents involving industrial control systems and online attackers, security experts are not looking at this discovery lightly given the kind of grave repercussions attacks like this pose to national security.

At the tail-end of 2015, the first malware-driven power outage was reported in Ukrainenews article, with the resurfacing of BlackEnergy, a malware package first seen in 2007. Earlier this month, the United States and the United Kingdom agreed to simulate cyber attacks on nuclear plants to gauge the two countries' readiness to take on threats that could affect nuclear plants.

Visit the Threat Intelligence Center for more on ICS and SCADA systems and industrial cyber security.

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.
