# Replication Through Removable Media, Technique T0847 - ICS

Archived: 2026-04-05 16:09:11 UTC

Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment. The adversary may rely on unknowing trusted third parties, such as suppliers or contractors with access privileges, to introduce the removable media. This technique enables initial access to target devices that never connect to untrusted networks, but are physically accessible.

Operators of the German nuclear power plant, Gundremmingen, discovered malware on a facility computer not connected to the internet. [1] [2] The malware included Conficker and W32.Ramnit, which were also found on eighteen removable disk drives in the facility. [3] [4] [5] [6] [7] [8] The plant has since checked for infection and cleaned up more than 1,000 computers. [9] An ESET researcher commented that internet disconnection does not guarantee system safety from infection or payload execution. [10]

---

Source: https://attack.mitre.org/techniques/T0847