ZeroCleare (Malware Family)

By Fraunhofer FKIE

ZeroCleare is a destructive malware. It has been developed in order to wipe the master boot record section in order to damage a disk's partitioning. Attackers use the EldoS RawDisk driver to perform the malicious action, which is not a signed driver and would therefore not runnable by default. The attackers managed to install it by using a vulnerable version of VBoxDrv driver, which the DSE accepts and runs. Used to attack middle-east energy and industrial sectors.

▶ [TLP:WHITE] win_zerocleare_auto (20251219 | Detects win.zerocleare.)
