Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:00:28 UTC

Description(SentinelOne) At first glance, HermeticWiper appears to be a custom-written application with very few standard functions. The malware sample is 114KBs in size and roughly 70% of that is composed of resources. The developers are using a tried and tested technique of wiper malware, abusing a benign partition management driver, in order to carry out the more damaging components of their attacks. Both the Lazarus Group (Destover) and APT33 (DistTrack) took advantage of Eldos RawDisk in order to get direct userland access to the filesystem without calling Windows APIs. HermeticWiper uses a similar technique by abusing a different driver, empntdrv.sys.
