LevelBlue - Open Threat Exchange

By TheNewRaikage

Archived: 2026-04-05 16:39:58 UTC

FileHash-SHA256: 5 | **IPv4:** 1 | **URL:** 4 | **YARA:** 2 | **Domain:** 2

Crooks behind MajikPOS have various tricks up their sleeves. Apart from infecting systems with it, we also spotted instances where common lateral movement tools were detected around the same time they were actively compromising the endpoint with MajikPOS. These tools include: HKTL_MIMIKATZ, HKTL_FGDUMP, and HKTL_VNCPASSVIEW. We surmise that the bad guys attempted to gain further access within the victim’s network. In separate isolated incidents, we also noticed the deployment of MajikPOS via PsExec, a command-line tool that can be used to remotely execute processes on other systems. This may indicate that valid, administrative level credentials were used against the host. The attackers also tend to deploy what works or what's convenient, as we’ve also seen them attempt to infect the target host with other PoS malware such as PwnPOS (TSPY_PWNPOS.SMA), and BlackPOS (TSPY_POCARDL.AI).
