PHOREAL (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:26:50 UTC

Phoreal is a very simple backdoor that is capable of creating a reverse shell, performing simple file I/O and top-level window enumeration. It communicates to a list of four preconfigured C2 servers via ICMP on port 53

▶ [TLP:WHITE] win_phoreal_auto (20251219 | Detects win.phoreal.)
