IRONHALO (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:06:34 UTC

IRONHALO is a downloader that uses the HTTP protocol to retrieve a Base64 encoded payload from a hard-coded command-and-control (CnC) server and uniform resource locator (URL) path.
The encoded payload is written to a temporary file, decoded and executed in a hidden window. The encoded and decoded payloads are written to files named igfxHK[%rand%].dat and igfxHK[%rand%].exe respectively, where [%rand%] is a 4-byte hexadecimal number based on the current timestamp. It persists by copying itself to the current user’s Startup folder.

▶ [TLP:WHITE] win_ironhalo_auto (20251219 | Detects win.ironhalo.)
