

# BUBBLEWRAP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:25:04 UTC

BUBBLEWRAP is a full-featured backdoor that is set to run when the system boots, and can communicate using HTTP, HTTPS, or a SOCKS proxy. This backdoor collects system information, including the operating system version and hostname, and includes functionality to check, upload, and register plugins that can further enhance its capabilities.

► [TLP:WHITE] win\_bubblewrap\_auto (20251219 | Detects win.bubblewrap.)

---

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.bubblewrap>