

CobInt (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:13:10 UTC

CobInt, is a self-developed backdoor of the Cobalt group. The modular tool has capabilities to collect initial intelligence information about the compromised machine and stream video from its desktop. If the operator decides that the system is of interest, the backdoor will download and launch CobaltStrike framework stager. It's CRM mailslot module was also observed being downloaded by ISFB.

► [TLP:WHITE] win_cobint_auto (20251219 | Detects win.cobint.)

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