# Karius (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 15:53:48 UTC

According to checkpoint, Karius is a banking trojan in development, borrowing code from Ramnit, Vawtrack as well as Trickbot, currently implementing webinject attacks only.

It comes with an injector that loads an intermediate "proxy" component, which in turn loads the actual banker component.

Communication with the c2 are in json format and encrypted with RC4 with a hardcoded key.

In the initial version, observed in March 2018, the webinjects were hardcoded in the binary, while in subsequent versions, they were received by the c2.

▶ [TLP:WHITE] win_karius_auto (20251219 | Detects win.karius.)

---