PandaBanker (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:35:56 UTC

According to Arbor, Forcepoint and Proofpoint, Panda is a variant of the well-known Zeus banking trojan(*). Fox IT discovered it in February 2016.

This banking trojan uses the infamous ATS (Automatic Transfer System/Scripts) to automate online bank portal actions.

The baseconfig (c2, crypto material, botnet name, version) is embedded in the malware itself. It then obtains a dynamic config from the c2, with further information about how to grab the webinjects and additional modules, such as vnc, backsocks and grabber.

Panda does have some DGA implemented, but according to Arbor, a bug prevents it from using it.

▶ [TLP:WHITE] win_pandabanker_auto (20251219 | Detects win.pandabanker.)
