BreachRAT (Malware Family)

By Fraunhofer FKIE

This is a backdoor which FireEye call the Breach Remote Administration Tool (BreachRAT), written in C++. The malware name is derived from the hardcoded PDB path found in the RAT: C:\Work\Breach Remote Administration Tool\Release\Client.pdb

▶ [TLP:WHITE] win_breach_rat_auto (20251219 | Detects win.breach_rat.)
