SodaMaster (Malware Family)

By Fraunhofer FKIE

This is a RAT that is usually loaded with one or more shellcode and/or reflective DLL injection techniques. The RAT uses RC4 or a hardcoded RSA key for traffic encryption/decryption. Its communication can either happen via a raw TCP socket or a HTTP POST request. Depending on the version, the RAT may remotely execute DLLs or shellcode.

▶ [TLP:WHITE] win_sodamaster_auto (20241030 | Detects win.sodamaster.)
