PocoDown (Malware Family)

By Fraunhofer FKIE

uses POCO C++ cross-platform library, Xor-based string obfuscation, SSL library code and string overlap with Xtunnel, infrastructure overlap with X-Agent, probably in use since mid-2018

▶ [TLP:WHITE] win_pocodown_auto (20251219 | Detects win.pocodown.)
