MagicRAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:32:21 UTC

According to Talos, MagicRAT is programmed in C++ programming language and uses the Qt Framework by statically linking it to the RAT on 32- and 64-bit versions. The Qt Framework is a programming library for developing graphical user interfaces, of which this RAT has none. Talos thinks that the objective was to increase the complexity of the code, thus making human analysis harder. On the other hand, since there are very few examples (if any) of malware programmed with Qt Framework, this also makes machine learning and heuristic analysis detection less reliable. The RAT uses the Qt classes throughout its entire code. The configuration is dynamically stored in a QSettings class eventually being saved to disk, a typical functionality provided by that class.

MagicRAT provides the operator with a remote shell on the victim's system for arbitrary command execution, along with the ability to rename, move and delete files on the endpoint. The operator can determine the timing for the implant to sleep, change the C2 URLs and delete the implant from the infected system.

▶ [TLP:WHITE] win_magic_rat_auto (20251219 | Detects win.magic_rat.)
