

Milum (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:04:55 UTC

In August 2019, Kaspersky Labs discovered a malware they dubbed Milum (naming based on internal file name fragments) when investigating an operation they named WildPressure. It is written in C++ using STL, primarily to parse JSON. Functionality includes bidirectional file transmission and remote command execution.

► [TLP:WHITE] win_milum_auto (20251219 | Detects win.milum.)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.milum>