AndroMut (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 12:46:03 UTC

According to Proofpoint, AndroMut is a new downloader malware written in C++ that Proofpoint researchers began observing in the wild in June 2019. The “Andro” part of the name comes from some of the pieces which bear resemblance to another downloader malware known as Andromeda [1] and “Mut” is based off a mutex that the analyzed sample creates: “mutshellmy777”.

▶ [TLP:WHITE] win_andromut_auto (20251219 | Detects win.andromut.)
