

Peppy RAT (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 17:51:43 UTC

Peppy is a Python-based RAT with the majority of its appearances having similarities or definite overlap with MSIL/Crimson appearances. Peppy communicates to its C&C over HTTP and utilizes SQLite for much of its internal functionality and tracking of exfiltrated files. The primary purpose of Peppy may be the automated exfiltration of potentially interesting files and keylogs. Once Peppy successfully communicates to its C&C, the keylogging and exfiltration of files using configurable search parameters begins. Files are exfiltrated using HTTP POST requests.

► [TLP:WHITE] win_peppy_rat_auto (20201014 | autogenerated rule brought to you by yara-signator)

Source: https://malpedia.caad.fkie.fraunhofer.de/details/win.peppy_rat