AgfSpy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 00:05:54 UTC

The agfSpy backdoor retrieves configuration and commands from its C&C server. These commands allow the backdoor to execute shell commands and send the execution results back to the server. It also enumerates directories and can list, upload, download, and execute files, among other functions. The capabilities of agfSpy are very similar to dneSpy, except each backdoor uses a different C&C server and various formats in message exchanges.

▶ [TLP:WHITE] win_agfspy_auto (20251219 | Detects win.agfspy.)
