DneSpy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 22:00:29 UTC

DneSpy collects information, takes screenshots, and downloads and executes the latest version of other malicious components in the infected system. The malware is designed to receive a “policy” file in JSON format with all the commands to execute. The policy file sent by the C&C server can be changed and updated over time, making dneSpy flexible and well-designed. The output of each executed command is zipped, encrypted, and exfiltrated to the C&C server. These characteristics make dneSpy a fully functional espionage backdoor.

▶ [TLP:WHITE] win_dnespy_auto (20251219 | Detects win.dnespy.)
