TONEDEAF (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 14:44:48 UTC

TONEDEAF is a backdoor that communicates with Command and Control servers using HTTP or DNS. Supported commands include system information collection, file upload, file download, and arbitrary shell command execution. When executed, this variant of TONEDEAF wrote encrypted data to two temporary files – temp.txt and temp2.txt – within the same directory of its execution.

▶ [TLP:WHITE] win_tonedeaf_auto (20251219 | Detects win.tonedeaf.)
