BEATDROP (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 18:38:16 UTC

According to Mandiant, BEATDROP is a downloader written in C that uses Atlassian's project management service Trello for C&C. BEATDROP uses Trello to store victim information and retrieve AES-encrypted shellcode payloads to be executed. BEATDROP then injects and executes downloaded payloads into a suspended process. Upon execution, BEATDROP maps a copy of ntdll.dll into memory to execute shellcode in its own process. The sample then creates a suspended thread with RtlCreateUserThread the thread points to NtCreateFile. The sample changes execution to shellcode and resumes the thread. The shellcode payload is retrieved from Trello and is targeted per victim. Once the payload has been retrieved, it is deleted from Trello.

▶ [TLP:WHITE] win_beatdrop_auto (20251219 | Detects win.beatdrop.)
