GEMCUTTER (Malware Family)

By Fraunhofer FKIE

According to FireEye, GEMCUTTER is used in a similar capacity as BACKBEND (downloader), but maintains persistence by creating a Windows registry run key.
GEMCUTTER checks for the presence of the mutex MicrosoftGMMZJ to ensure only one copy of GEMCUTTER is executing. If the mutex doesn't exist, the malware creates it and continues execution; otherwise, the malware signals the MicrosoftGMMExit event.

▶ [TLP:WHITE] win_gemcutter_auto (20251219 | Detects win.gemcutter.)
