LiteDuke (Malware Family)

By Fraunhofer FKIE

According to CarbonBlack, LiteDuke is a third stage backdoor. It appears to use the same dropper as PolyglotDuke. Its payload makes use of an AES encrypted SQLite database to store its configuration. LiteDuke supports a large number of individual commands including host information retrieval, file upload and download, and the ability to execute other code. LiteDuke C2 servers appear to be compromised servers, and the malware communicates with them using normal HTTP requests. It attempts to use a realistic User-Agent string to blend in better with normal HTTP traffic.
ESET have dubbed it LiteDuke because it uses SQLite to store information such as its configuration.

▶ [TLP:WHITE] win_liteduke_auto (20251219 | Detects win.liteduke.)
