BabyShark (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:42:35 UTC

BabyShark is Microsoft Visual Basic (VB) script-based malware family first seen in November 2018. The malware is launched by executing the first stage HTA from a remote location, thus it can be delivered via different file types including PE files as well as malicious documents. It exfiltrates system information to C2 server, maintains persistence on the system, and waits for further instruction from the operator

▶ [TLP:WHITE] win_babyshark_auto (20251219 | Detects win.babyshark.)
