PinchDuke (Malware Family)

By Fraunhofer FKIE

According to F-Secure, the PinchDuke information stealer gathers system configuration information, steals user credentials, and collects user files from the compromised host transferring these via HTTP(S) to a C&C server. F-Secure believes that PinchDuke's credential stealing functionality is based on the source code of the Pinch credential stealing malware (also known as LdPinch) that was developed in the early 2000s and has later been openly distributed on underground forums.

▶ [TLP:WHITE] win_pinchduke_auto (20251219 | Detects win.pinchduke.)
