Dyre (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 23:38:43 UTC

The Dyre Banking Trojan, discovered in June 2014, targets online banking websites for credential theft and fraud. It uses a man-in-the-browser approach, encryption, and spam emails for distribution.

Dyre's architecture includes a dropper and main DLL module, with techniques for persistence and evasion. Its command and control infrastructure is hidden through proxies, and it can adapt using a domain generation algorithm and I2P integration. Researchers have linked Dyre to the Gozi and Neverquest families.

▶ [TLP:WHITE] win_dyre_auto (20251219 | Detects win.dyre.)
