Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:37:59 UTC

Description(Trend Micro) Developed in 2016, TrickBot is one of the more recent banking Trojans, with many of its original features inspired by Dyreza (another banking Trojan). Besides targeting a wide array of international banks via its webinjects, Trickbot can also steal from Bitcoin wallets.

Some of its other capabilities include harvesting emails and credentials using the Mimikatz tool. Its authors also show an ability for constant new features and developments.

Trojan.TrickBot comes in modules accompanied by a configuration file. Each module has a specific task like gaining persistence, propagation, stealing credentials, encryption, and so on. The C&Cs are set up on hacked wireless routers.

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=1ee83664-1baa-49f4-8056-c9a2d73a9a80