TinyNuke (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 19:46:40 UTC

TinyNuke (aka Nuclear Bot) is a fully-fledged banking trojan including HiddenDesktop/VNC server and a reverse socks4 server. It was for sale on underground marketplaces for $2500 in 2016. The program's author claimed the malware was written from scratch, but that it functioned similarly to the ZeuS banking trojan in that it could steal passwords and inject arbitrary content when victims visited banking Web sites. However, he then proceeded to destroy his own reputation on hacker forums by promoting his development too aggressively. As a displacement activity, he published his source code on Github. XBot is an off-spring of TinyNuke, but very similar to its ancestor.

▶ [TLP:WHITE] win_tinynuke_auto (20251219 | Detects win.tinynuke.)
