Small banking Trojan poses major risk

By John Leyden

Published: 2012-06-04 · Archived: 2026-04-05 13:45:13 UTC

Security researchers have discovered a tiny, but highly capable banking Trojan.

Tinba (Tiny Banker, or otherwise known as Zusy) hooks itself into browsers before stealing banking login information and snaffling network traffic.

The malware used injected code and Man in The Browser (MiTB) tricks to change the way banking websites are presented to victims on compromised machines.

The technique is designed to thwart added security protections, most specifically two-factor authentication technologies, that have come into deployment by some banks. ZeuS, the well-established banking Trojan, uses much the same trickery to achieve the same nefarious ends.

Weighing in at just 20KB, Tinba represents a new family of banking Trojan. Antivirus detection of the analyzed samples is low, according to researchers at CSIS Security, a Danish firm.

Tinba uses a RC4 encryption scheme when communication with its Command & Control (C&C) servers, located at four hardcoded domains. "Tinba proves that malware with data stealing capabilities does not have to be 20MB of size," Peter Kruse, a researcher with CSIS, told *El Reg*.

His comments reference the avalanche of publicity that has accompanied the discovery of the Flame cyber-espionage toolkit, a portly 20MB chiefly notable for affecting systems in Iran and the ability to turn its worm like propagation routines on and off for added stealth.

CSIS has a detailed write-up of Tinba here. ®
