

Mispadu (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:10:08 UTC

According to ESET Research, Mispadu is an ambitious Latin American banking trojan that utilizes McDonald's malvertising and extends its attack surface to web browsers. It is used to target the general public and its main goals are monetary and credential theft. In Brazil, ESET has seen it distributing a malicious Google Chrome extension that attempts to steal credit card data and online banking data, and that compromises the Boletto payment system.

► [TLP:WHITE] win_mispadu_auto (20201014 | autogenerated rule brought to you by yara-signator)

Source: <https://malpedia.caad.fkie.fraunhofer.de/details/win.mispadu>