

Banking Trojan Zeus Panda shambles into Brazil ahead of Olympics

By Devin Coldewey

Published: 2016-08-04 · Archived: 2026-04-05 20:44:59 UTC

11:38 AM PDT · August 4, 2016

It seems there's no limit to the perils being faced by athletes at the Rio 2016 Olympics: not just their competitors, but toxic water, poor accommodations and impressive mobile bills. Add malicious pandas to the menu — virtual ones, at least. A nasty Trojan known as Zeus Panda has [made its way to the Olympic host](#) just in time for an influx of visitors.

IBM's X-Force Research discovered that the Trojan, a variant of the Zeus variety that's been kicking around for the last few years, had spread to Brazil in July. Zeus and its relatives — the pantheon, if you will — target transactions such as online banking logins, payment portals and bitcoin exchanges. Basically anywhere they can slip in and steal a login with the power to approve more such transactions.

The specifics of this Panda variant are [discussed here by Arbor Networks](#). It seems to be largely the same as previous malware in this lineage, albeit modified to frustrate the latest detection packages and target Brazilian banks and services specifically.

Deployment appears to be done professionally, as well — the Trojan is likely being sold in the usual nooks of the Dark Net where such sundries are found. So far the preferred delivery mechanism has been Word docs with embedded code that activates the malware, but other vectors are of course in play, as well. One-time passwords for two-factor authentication are acquired via a fraudulent 2FA pop-up that forwards that data on to the hackers.

IBM notes that the software behind Zeus Panda isn't particularly new, nor is the cybercrime scene in Brazil particularly advanced — so Panda may be as a wolf (or rather bear) among lambs.

You can avoid Trojans like this by not opening strange attachments or following suspicious links, but it can also be addressed at a systematic level by the banks being targeted. The methodology of this malicious software is well understood, but it takes vigilance (and savvy IT) to keep it at bay.

Topics

Devin Coldewey is a Seattle-based writer and photographer.

His personal website is coldewey.cc.

[View Bio](#) >

Source: <https://techcrunch.com/2016/08/04/banking-trojan-zeus-panda-shambles-into-brazil-ahead-of-olympics/>