

# After Panda Comes the Sphinx

 [securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/](https://securityintelligence.com/brazil-cant-catch-a-break-after-panda-comes-the-sphinx/)

August 16, 2016



Malware August 16, 2016

By [Limor Kessem](#) co-authored by [Denis Laskov](#) , [Ziv Eli](#) 4 min read

Within two weeks of the [discovery of Zeus Panda \(Panda Banker\)](#) activity, IBM X-Force researchers have uncovered the first signs of Zeus Sphinx attacks in Brazil. A new version of Zeus Sphinx, which is, like Panda, also a commercially available Zeus v2 variation, now targets the online banking and Boleto payment services of three of the top Brazilian banks and one bank in Colombia, according to its configuration file.

Sphinx is a modular banking Trojan and considered to be as sophisticated as Panda and Zeus Citadel. The timing of Sphinx's migration to Brazil — while the country is hosting a global sporting event — hardly appears to be a coincidence. Cybercriminals are known to increase their efforts during sporting events, taking advantage of the rise in online activity and interest around the competition to lure users into opening malware spam and phishing pages.

## **Sphinx: Mythically Treacherous and Double-Edged**

---

Zeus Sphinx is a banking Trojan and is a commercial offering sold to cybercriminals via underground fraudster boards. The malware emerged in August 2015, at which point it started [targeting major banks in the U.K.](#) This malware was known to primarily target European entities until recently.

So, another day, another Zeus? Not quite. Sphinx has been around for about a year now, launched initially in attacks targeting U.K. and Australian banks. X-Force Research analyzed Sphinx's modus operandi at the time and found that the malware combined elaborate fraud tactics to steal credentials and one-time passwords.

Sphinx's configuration fetched webinjections in real time from its command-and-control (C&C) server, manipulated users to generate authentication codes with their card readers and even tricked victims into downloading a malware app to their mobile device to steal transaction authentication codes sent from the bank via SMS.

## **Boleto Fraud Costs Brazilians Billions**

---

According to X-Force researchers, the Brazilian iteration of Zeus Sphinx, which is dubbed Sphinx v2, most likely comes from the same developer and is customized to target local banks. Aside from social engineering injections that ask for payment card PIN codes and PII, Sphinx v2 has been adapted to rob Boleto payments from infected victims. For those that aren't familiar with Boleto payments, think of them as something similar to a money order in the U.S.

According to X-Force researchers, [Boletos have been a lucrative target](#) for Brazilian malware authors for the past few years, with one estimate [attributing \\$3.75 billion](#) in fraud losses to just one cybercrime faction that targeted Brazilians from 2012 to 2014.

## How Boleto Fraud Works

---

The typical Boleto fraud malware is facilitated by various codes, which are specifically designed to poison and rob payments from infected user endpoints. But in the case of Zeus Sphinx v2, stealing Boletos is just one of the malware's preconfigured theft mechanisms, enabled by real-time man-in-the-middle (MitM) webinjections.

The Boleto fraud begins when infected users initiate a Boleto Bancario during their online banking session. At that moment, the malware identifies that a Boleto is being prepared and triggers a set of JavaScript injections.

**Related:** [Panda Is One Hungry Bear! A Heavyweight Banking Trojan Rolls Into Brazil](#)  
Sphinx collects the victim's Boleto data and sends it to the criminal's C&C. On the server side, the C&C reaches out to a legitimate open source API library that creates Boleto barcodes from transaction details defined by the user. This happens without involving the bank's server, where the victim's original Boleto barcode should come from. Instead, the criminal-generated barcode contains the routing data to a mule account and a modified transfer amount.

Since the barcode is not readable by humans, the victim cannot tell there is any issue with the barcode response that appears to come from the bank. Ultimately, the rendered barcode the victim unknowingly sends out is the poisoned Boleto request, which effectively reroutes the payment to the criminal. This Sphinx feature automates the fraud and does not require manual intervention from the cybercriminal behind the malware until the actual cashing out of the Boleto payment.

## A Mythical Beast Running the Streets

---

Zeus Sphinx, which is based on the [leaked source code](#) of the Zeus Trojan, targets retail banking and Boleto payments of banks in Brazil and Colombia. The malware adapts social engineering injections to manipulate users in each targeted bank. While in some cases Sphinx webinjections only ask victims to provide passcodes and PII, in others it also requires payment card PIN codes as well as the person's home and mobile phone numbers.

The latter case is interesting because it tells the story of fraud that's typical to Brazil: mixing digital and physical social engineering to scam victims and empty their accounts. In these schemes, fraudsters may start off the chain by stealing online banking details. Then, to obtain more information, they may supplement their scams with phone calls to the victims.

## An Active and Evolving Project

---

After the recent spread of Zeus Panda to Brazil, Sphinx's move to the country may mark the beginning of a trend that will add to [Brazil's existing cybercrime threats](#) — a landscape that has been, until now, dominated by relatively simplistic Delphi-based malcode.

This migration of yet another commercial Zeus variant into Brazil further underscores the trending collaboration between Brazil-based cybercriminals and cybercrime vendors from other countries and underground communities — a movement that has been picking up speed in the country since the beginning of 2016.

Judging by recent emerging campaigns observed by X-Force Research, Zeus Sphinx appears to be an active and evolving project, commercialized to cybercriminals through Dark Web forums. As such, we may see more variations of this malware in the coming months and an expanding list of targets in Brazil.

## Striking Down Zeus Sphinx Attacks

---

IBM Security is familiar with Zeus Sphinx and its various attack schemes. To help thwart Sphinx, banks can use adaptive [malware detection solutions](#) and [protect customer endpoints](#) with malware intelligence that provides real-time insight into fraudster techniques and capabilities.

To prevent malware infections on their endpoints, users should make sure their operating system and frequently used programs are up to date at all times. When browsing, users should disable ads and avoid sites typically prone to infection, such as those hosting adult content, torrents and free gaming. Most importantly, users should avoid clicking on links or attachments in unsolicited email.

## Sample MD5

---

A sample MD5 hash for the Zeus Sphinx Trojan is 03915A1F03DF164F48AC4DFD04D9C2C4. Antivirus aliases include Trojan-Spy.Win32.Zbot, according to [VirusTotal](#).

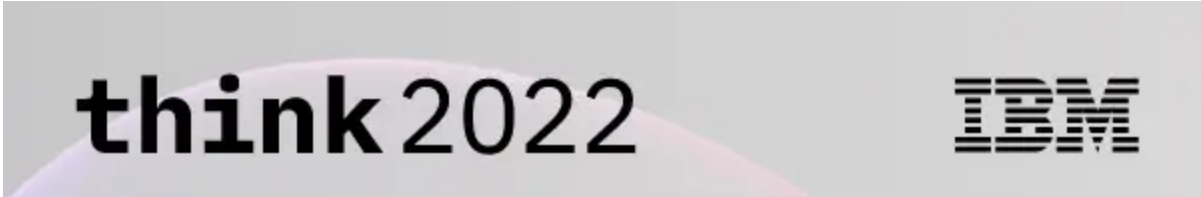
IBM X-Force Research will be updating information and IOCs on Zeus Sphinx via the [X-Force Exchange platform](#). Join XFE today to keep up to date regarding this threat and other findings from our cybercrime labs.

[Read the white paper: Accelerating growth and digital adoption with seamless identity trust](#)

[Limor Kessem](#)

Executive Security Advisor, IBM

Limor Kessem is an Executive Security Advisor at IBM Security. She is a widely sought-after security expert, speaker and author and a strong advocate for wom...



think 2022



IBM

IBM Think Broadcast  
Let's think together.

Watch on demand →

