

Zeus Sphinx Pushes Empty Configuration Files — What Has the Sphinx Got Cooking?

 securityintelligence.com/zeus-sphinx-pushes-empty-configuration-files-what-has-the-sphinx-got-cooking/

June 15, 2017



[Home](#) / [Banking & Finance](#)

Zeus Sphinx Pushes Empty Configuration Files — What Has the Sphinx Got Cooking?



[Banking & Finance](#) June 15, 2017

By [Limor Kessem](#) 3 min read

Lately, [IBM X-Force Research](#) has seen the Zeus Sphinx Trojan go through a targetless phase, an exceedingly rare occurrence in the cybercrime arena.

Recent Zeus Sphinx samples have fetched configuration files in which all the target URLs were removed. This means that while Sphinx infection campaigns continue and the malware can infect new machines, it remains idle and lacks attack instructions to target specific banks and banking services.

The only instruction that repeats in all Sphinx configuration is to inject a victim's "bot ID" into every page he or she visits. In essence, this is a webinjection attack: Inject into `http*://*`, covering any HTTP and HTTPS webpage the victim browses to.

[Read the white paper: Shifting the balance of power with cognitive fraud prevention](#)

What's Cooking?

This phase of empty Sphinx configuration files started in March 2017 and increased over the past few months to include all Sphinx samples. This suggests that Sphinx is presently operated by one group, not multiple actors, despite the fact that it was commercially sold in the underground when it was launched in 2015. What are Sphinx's operators cooking up?

In 2017, the malware was [targeting banks](#) in a number of countries, mostly focusing on Australia, the U.S. and Canada. Throughout that time, and to date, Sphinx's operators have launched different infection campaigns to spread the malware to more users.

According to X-Force research, one of the most interesting phases came in late January 2017, when Sphinx was being delivered by a well-known spam source called Moskalvzapoe. This network was one of the more prominent distributors of the Neverquest Trojan, serving spam for cybercriminal customers.

A notable change came in the week of Jan. 19 to Jan. 24, 2017, when Neverquest delivery via Moskalvzapoe suddenly halted. After that week, Moskalvzapoe got right back into serving banking Trojans, only this time it was spreading Zeus Sphinx, dropping it via Moskalvzapoe's DEXLoader, also known as Terdot.

Neverquest has since completely died down, dropping from the second most prevalent financial malware families into oblivion. Zeus Sphinx, on the other hand, has been climbing up the chart ever since, placing fifth in June, right under seasoned organized cybercrime gangs such as Gozi, Ramnit and Dridex, per X-Force data.



Figure 1: Top most prevalent financial malware families (Source: IBM X-Force, June 2017 YTD)

Did the Neverquest gang take over Sphinx after the arrest of one of its members? What is the purpose of injecting a bot ID into each page visited by infected users? Are the Sphinx operators planning to set up the botnet for monetization, similar to how Neverquest used to rent botnet sections to the cybercrime elite?

These questions will likely remain unanswered until the next change takes place. And while the botnet continues to amass new infections, at least banking customers are getting a break for the time being.

At this time, Sphinx does not have defined targets, but X-Force data revealed that recent campaigns have affected users in North America, the U.K. and Australia. It is possible that Sphinx's operators are preparing new targets, sectioning the botnet or partnering with other groups, and will go back to targeting the banking sector in the coming weeks.

About Sphinx

Zeus Sphinx originally emerged in 2015, when it was up for sale in the Russian-speaking underground by a vendor who apparently picked up the Zeus v2 source code and commercialized it. The first Sphinx attacks were configured to target PayPal, banks in the U.K. and a bank in Poland using elaborate webinjections to trick victims into authorizing fraudulent transactions.

The malware, which was most likely operated by different actors, started popping up in other geographies, most notably Brazil and Colombia, in the summer of 2016. At the time, Sphinx was adapted to the Brazilian financial sector with more than just local targets, also adding

Boleto payment manipulation to the mix. Boleto payments are very popular in Brazil — they are similar to the money order concept in the U.S. — and Sphinx featured a module that automatically rerouted these payments to its operators.

X-Force data revealed that by January 2017, the malware started targeting banks in Canada and Australia, increasing its activity in the surrounding areas, particularly New Zealand and the U.S. In March, Sphinx saw all URL targets removed from some configurations, eventually affecting all Sphinx configurations fetched by infected bots in the second quarter of 2017.

Sample IoCs

Below are sample indicators of compromise (IoCs) used in this report:

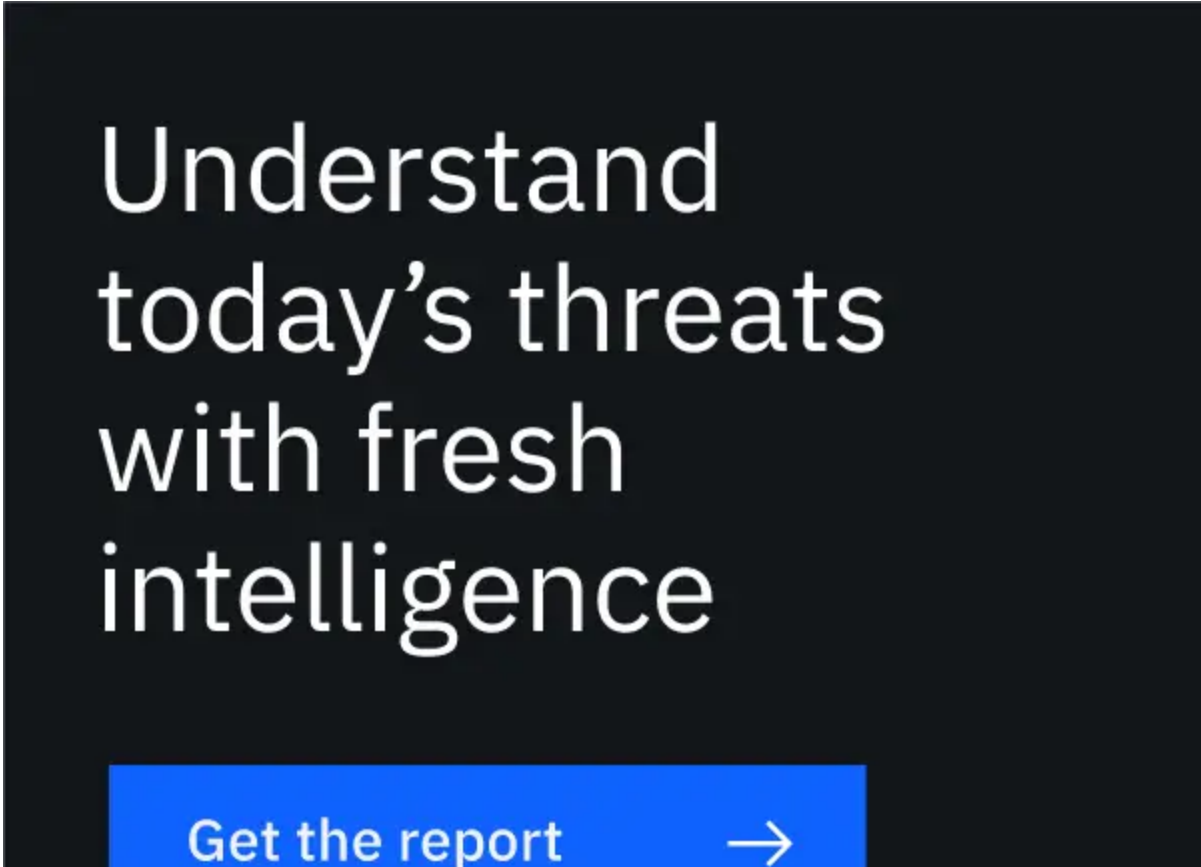
- Sphinx dropper MD5: 03C6126B88F9BB51F80C5C370CE233CD
- Sphinx sample MD5: 070134AAAF7E64DF29C2D94F8CF94BF9
- Sphinx empty configuration MD5: 0235990b83a976fd0aed8202a527b65c

[Read the white paper: Prevent phishing success with cognitive fraud detection](#)

[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...



Understand
today's threats
with fresh
intelligence

Get the report





IBM Security