From Canada to Australia and Back

securityintelligence.com/around-the-world-with-zeus-sphinx-from-canada-to-australia-and-back/

January 26, 2017

Home / Banking & Finance

Around the World With Zeus Sphinx: From Canada to Australia and Back

Banking & Finance January 26, 2017
By Limor Kessem 3 min read

IBM X-Force researchers recently identified new infection campaigns delivering distinct Zeus Sphinx Trojan variants to online banking users in Canada and Australia. This is the first time our researchers have observed Sphinx campaigns with dedicated configurations targeting financial institutions in either of the two countries. We believe they are part of ongoing testing by Sphinx operators.

Sphinx has been keeping low levels of activity since August 2016, when it was detected in attacks on Brazilian banks. The malware authors have been making small, incremental upgrades to the code.

The recent configurations targeting online banking consumers in Canada and Australia are used sparingly in what looks like low-volume testing, not full-blown infection campaigns. The malware's operators appear to be looking very carefully to determine which geographies offer the paths of least resistance.

Zeus Sphinx Targets Banks in Canada and Australia

In Canada, Sphinx's operators included URLs for over 33 financial institutes. They focused their target list on credit unions, likely seeing them as the lower hanging fruit in the Canadian financial sector. The malware's targets are consumer accounts.

Figure 1: Sphinx's Canadian target distribution per entity type (Source: IBM X-Force)

The Canada-focused Sphinx operators are most likely familiar with the cybercrime arena. According to our research team, they used the same attack servers that facilitated the Zeus Citadel and Ramnit attacks in early 2016 and the fourth quarter of 2016, respectively. The webinjections share familiar code patterns with other banking Trojans, indicating that the attackers likely bought them from an injection-writing service.

Familiar Tricks

In their recent campaigns, Sphinx's operators have been using two distribution methods to spread the malware to new victims: email messages containing malicious Word documents that launch a visual basic for applications (VBA) loader and malvertising schemes designed to spread the Sundown exploit kit (EK).

The use of the Sundown EK provides further evidence that Sphinx's operators may be linked to other commercial malware operators. Sundown has been evolving since the fourth quarter of 2016, from a relatively small, second-tier kit into one of the most prominent EKs in circulation. It includes older exploits for Internet Explorer, Flash and Silverlight. It has been previously connected with other banking Trojans such as Kronos and with previous malware campaigns in Canada.

In Australia, the configuration targets a mix of 40 major banks, credit unions and payment providers. That configuration also targets some banks based in the U.S.


Figure 2: Sphinx's Australia-focused target distribution per geo (Source: IBM X-Force)

IBM X-Force research reported past Sphinx campaigns launched against Brazilian banks in 2015 and U.K. banks in 2016.

Financial Malware: A Global Perspective

From a global perspective, Sphinx is counted as part of the overall Zeus family of Trojans, since it is almost entirely based on the leaked Zeus v2.0.8.9 source code.

With multiple Zeus variations such as Panda, Sphinx and Floki Bot active in the wild, Zeus's codebase maintains the top position as the most active banking Trojan family. Different variants are operated by numerous cybercrime factions worldwide.


Figure 3: Most prevalent financial malware families 2017 YTD (Source: IBM X-Force)

Relevant IoCs

IBM X-Force shares Zeus Sphinx indicators of compromise (IoCs) on IBM X-Force Exchange. Just type “Zeus Sphinx” into the search bar to find all related collections on this malware.

Your team can anonymously add to Zeus Sphinx collections by sharing additional IoCs on X-Force Exchange. This ultimately helps information security professionals fight cybercrime threats in closer to real time, cutting malware’s lifelines.

To share and follow Zeus Sphinx IoCs, check out the dedicated collection on X-Force Exchange.

Dropper MD5

33DAE99769B84EFCE58C6EBD0B5C8626

Sample MD5

Sample MD5 hashes are:

- C5ADC8EC369941CDF3DFC6B4E8BC799C
- 7B83DFCC671C5210F5A8A1D6552BADE4
- 57B083B80CE77D6F1AE37F59BD28B4B2

Mitigating Zeus Sphinx Attacks

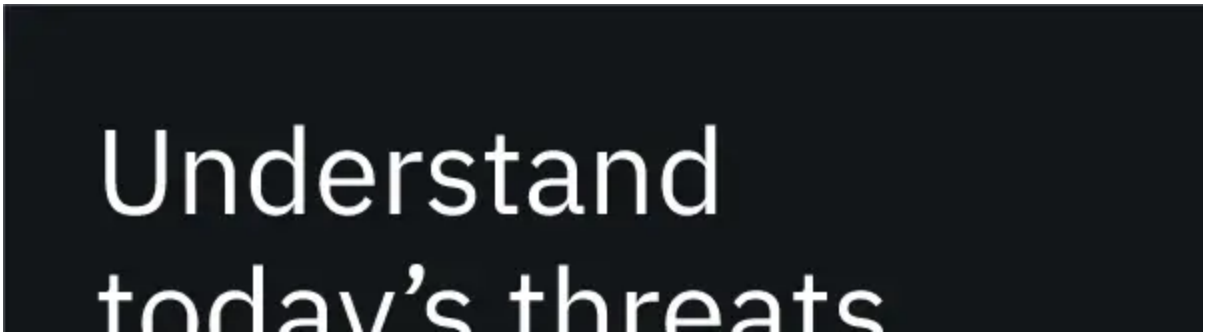
Banks wishing to protect their customers from evolving threats and cybercrime modus operandi are invited to learn more about IBM Trusteer Advanced Fraud Protection.

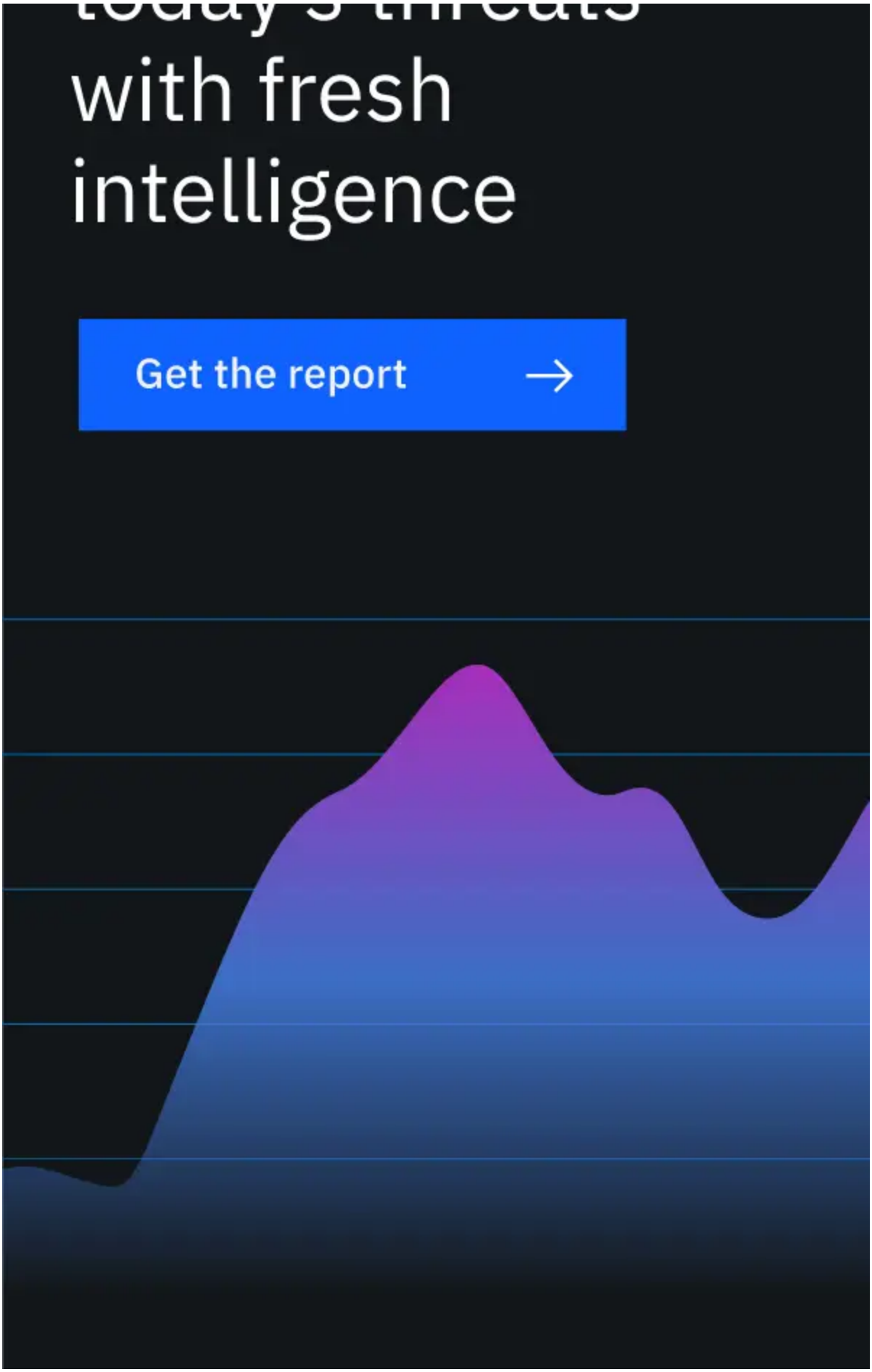
Individuals can reference our tips page for ways to protect themselves from malware such as Zeus Sphinx and other banking Trojans.

Read the white paper: How to outsmart Fraudsters 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...




with fresh
intelligence
Get the report


IBM Security