Banking Malware Spreading via COVID-19 Relief Payment Phishing

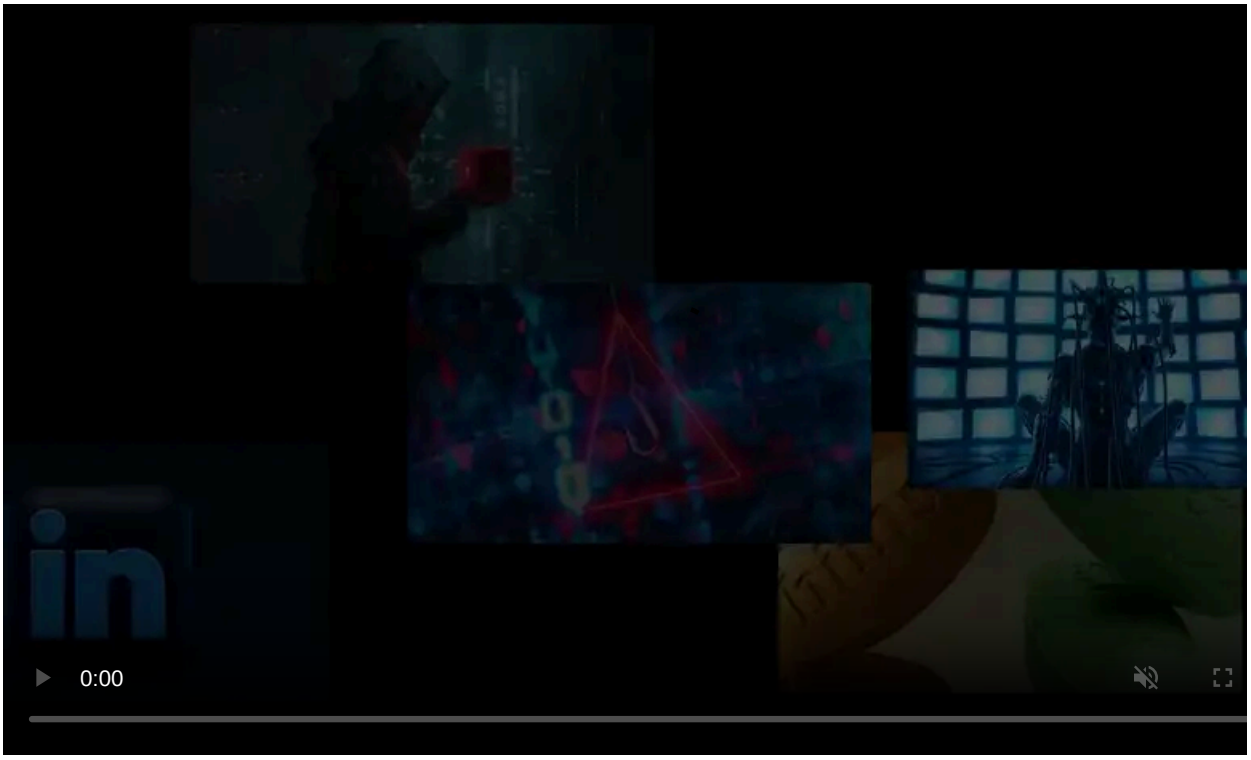
By Sergiu Gatlan

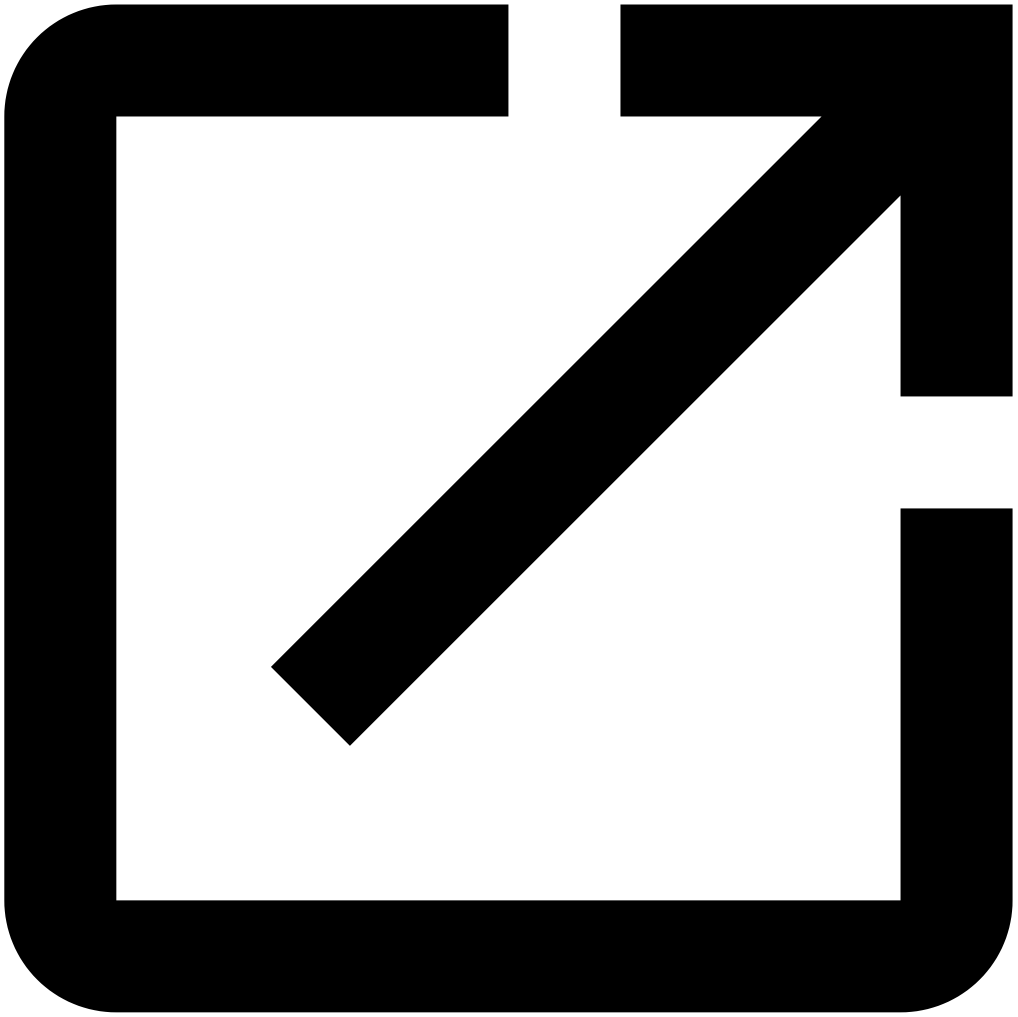
Published: 2020-03-30 · Archived: 2026-04-05 16:36:50 UTC

The Zeus Sphinx banking Trojan has recently resurfaced after a three years hiatus as part of a coronavirus-themed phishing campaign, the most common theme behind most attacks by far during the current pandemic.

Zeus Sphinx (also known as Zloader and Terdot) is a malware strain that was initially spotted back in August 2015 when its operators used it to attack several British financial targets and it is almost entirely based on the Zeus v2 Trojan's leaked source code (just as Zeus Panda and Floki Bot).

This malware was later used in attacks targeting banks from all over the globe, from Australia and Brazil to North America, attempting to harvest financial data via web injections that make use of social engineering to convince infected users to hand out auth codes and credentials.


0:00

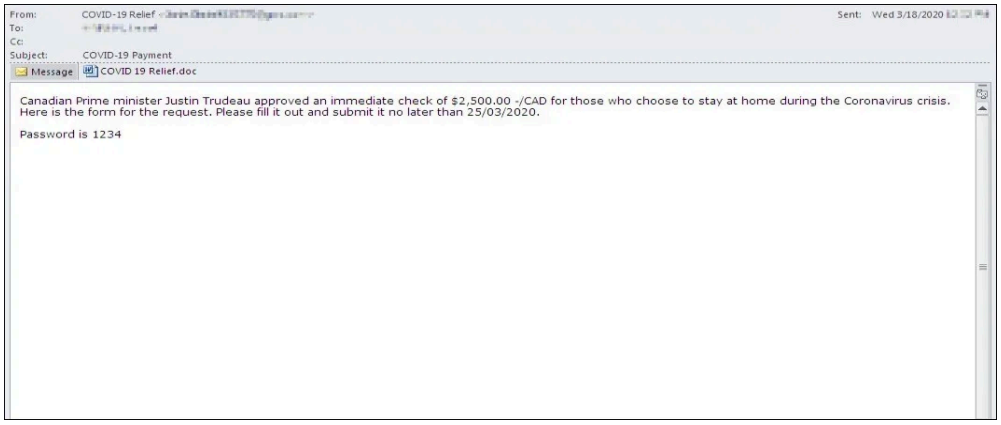


Back after a three-year break

The ongoing Zeus Sphinx campaign uses phishing emails that come with malicious documents designed to look like documents with information on government relief payments.

"While some Sphinx activity we detected trickled in starting December 2019, campaigns have only increased in volume in March 2020, possibly due to a testing period by Sphinx's operators," as IBM X-Force researchers Amir Gandler and Limor Kessem found.

"It appears that, taking advantage of the current climate, Sphinx's operators are setting their sights on those waiting for government relief payments."



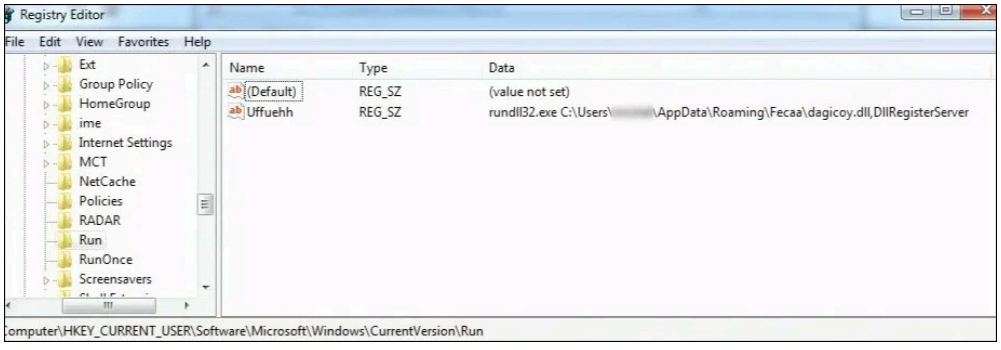
Phishing email sample (*IBM X-Force*)

Just as they did in previous campaigns, Sphinx's operators are still focusing their efforts on targets using major banks from the US, Canada, and Australia.

The attackers ask the potential victims to fill out a password-protected request form delivered in the form of a .DOC or .DOCX document. After submission, this should allow them to receive relief payments designed to help them out while staying at home.

Once opened on the targets' computer, these malicious documents will ask for macros to be enabled and infect them with the Sphinx banking Trojan after installing a malware downloader that fetches the final payload from a remote command-and-control (C&C) server.

After the victims' systems are compromised, Sphinx gains persistence and saves its configuration by adding several Registry keys and writing data in folders created under %APPDATA%.



Registry entry created to gain persistence (*IBM X-Force*)

"To carry out web injections, the malware patches explorer.exe and browser processes iexplorer.exe/chrome.exe/firefox.exe but doesn't have the actual capability of repatching itself again if that patch is fixed, which makes the issue less persistent and unlikely to survive version upgrades," the researchers also discovered.

Sphinx uses Tables web-based control panels for web injects and it will download custom files designed to match the websites of the victims' banks for the injections to be as convincing as possible.

The malware uses the web injects to alter the banks' websites to trick the victims into entering their credentials and authentication codes in forms that will exfiltrate the information to attacker-controlled servers.

One of many

This campaign is just one of an increasing number of others that try to exploit the COVID-19 pandemic by stealing sensitive information and infecting their targets with malware.

For instance, in somewhat related news, FBI's Internet Crime Complaint Center (IC3) warned that a phishing campaign was using fake government economic stimulus checks to steal personal info from victims.

To avoid getting scammed, infected with malware, or have your information stolen, IC3 recommends not clicking on links or opening attachments sent by people you don't know, as well as to make sure that the sites you visit are legitimate by typing their address in the browser instead of clicking hyperlinks embedded in emails.

You should also never provide sensitive info like user credentials or any type of financial data when asked as part of a telemarketing call or over email.
