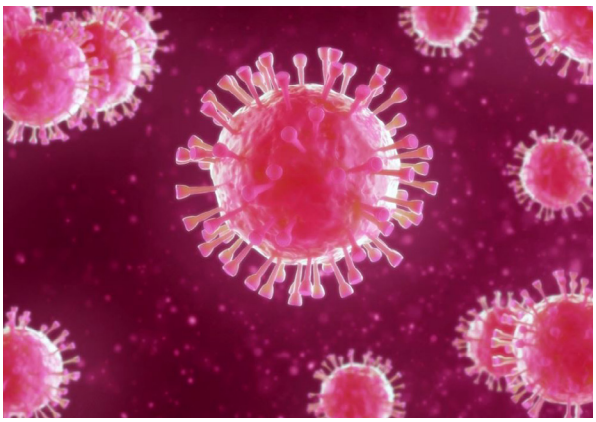
# LokiBot Rides Fear of Coronavirus



## Overview

During the first week of March, LokiBot infostealer joined the list of malware being distributed by threat actor(s) taking advantage of the fear and interest in the spread of Coronavirus (COVID-19). From 3 to 6 March, we observed two malicious spam (malspam) email campaigns distributing LokiBot under the guise of providing information on Coronavirus' impact on supply chains.

## Customer Impact

LokiBot has become a popular information stealer that collects credentials and security tokens from infected machines. Its code was leaked soon after it was first seen in 2015, which made it easy to modify and sell. LokiBot targets multiple applications, including but not limited to Mozilla Firefox, Google Chrome, Thunderbird, as well as FTP.

## Campaign Analysis

Threat actors behind LokiBot regularly use attachments that are archived files,[1] notably RAR, TAR and GZ file types. In previous Lokibot campaigns, we have seen threat actors use LZH and ISO files as well for their attachments. In one of our recent samples, the filename had a double extension; an attempt to make it appear to be a PDF file, rather than a TAR file.

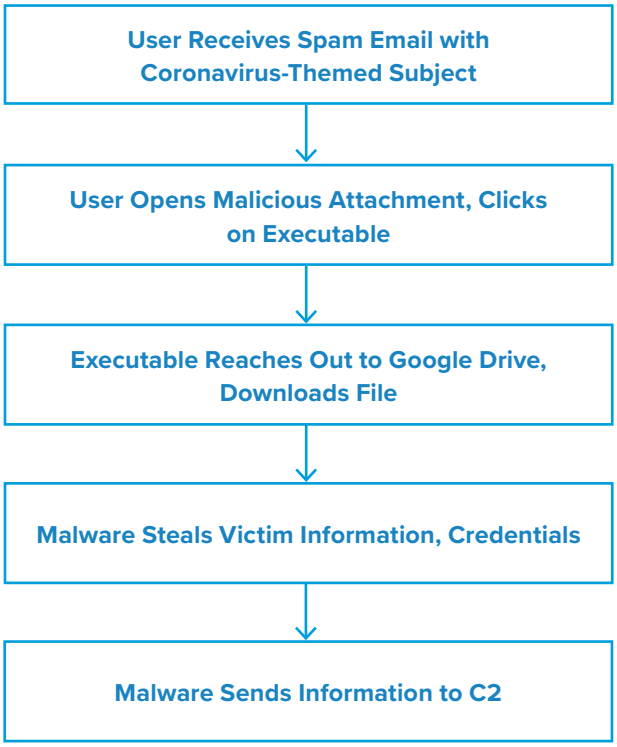
The email messages of the main campaign had two subject lines, one of which alleged to be a supply chain update in the context of Coronavirus (COVID-19). The other subject had a more typical payment transfer theme. Both sets of messages had attached files with the same filename (GEE CustomerUpdate English Corona 27022020..rar) and same SHA256 hash.

The second campaign we observed also had a logistical theme, claiming to outline the Coronavirus' impact to sea freight supply chains. The attached file was a TAR archive whose name made it appear to be a PDF: CoVid19_BAH.PDF.tar.

## Attack Chain

The larger LokiBot campaign that we found followed the same attack chain we described in our mid-February report on related SWIFT-themed campaigns, one of which distributed LokiBot.[2] Once the recipient opens the attached archive file and clicks on the executable, it reaches out to a Google Drive and downloads a file matching the naming pattern from February's campaign. The malware then steals the victim's information and sends it to a command and control (C2) server.

The sample from the second campaign did not execute after failing to receive a response to an initial attempt to reach out to a specific domain.




## Vulnerabilities & Mitigation

Threat actors use current event-themed subject lines to lure recipients into opening messages and uncompressing the attached files. As such, we recommend the following actions to reduce the risk of infection from malicious spam:

- Regularly train users to be aware of potential phishing efforts and how to handle them properly.
- Always be suspicious of unexpected and vague emails and unknown senders.
- Do not open files attached to emails that are suspicious or from unknown senders.
- Exercise additional caution when unexpected messages or attachments have commonly-used themes such as shipping or financial documents or advice.
- Verify important or potentially legitimate attachments with the sender via alternative means such as a phone call or separate email to a known contact.
- Check order statuses by browsing directly to the delivery website, rather than using an embedded link.

### Endnotes

1. https://en.wikipedia.org/wiki/List_of_archive_formats
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--58