allot
See. Control. Secure.

Coronavirus Alarm Report

April 2020

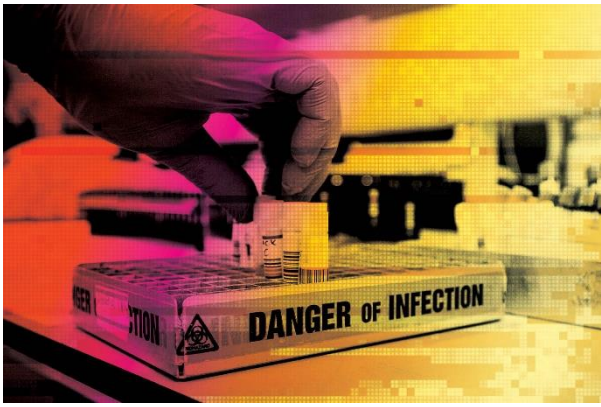
See. Control. Secure.

Contents

1 Introduction

This report is based on coronavirus-related data and the cyber protection information gathered during this event. It covers some of the **most important threats** using the coronavirus crisis, as well as research on these threats as they relate to our platform and how we are protecting our customers.

2 Why? How?



As mentioned in previous reports, cybercriminals will take advantage of any event that allows them to profit from malicious actions.

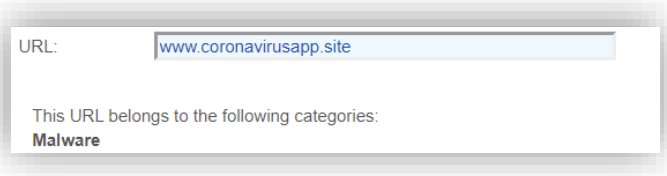
We are currently living through a **very tragic and unprecedented worldwide coronavirus crisis**. Sadly, this is also being used by ruthless cybercriminals. However, compared to other events that draw a lot of public attention (sports events, concerts, etc.), in this case, cybercriminals use “fear” to create a sense of urgency to reduce security awareness among victims. Doing so, the victim will fall more easily into their trap.

The most common methods used in order to trick the victims are the following:

- **Phishing**
- **E-mails containing malware,** hidden in documents
- **Malware downloads** through apparently “legitimate” websites

3 Malware downloaded through “legitimate” Websites

Let’s start with the least common method related with the coronavirus event. Cyber criminals **disguise malicious websites as legitimate ones** that host viruses, trying to trick the user to download.



- **CovidLock** is ransomware disguised as an Android application that showed a COVID-19 global heat map.
- Discovered March 16, 2020, it was intro-duced into our database just a day later.
- The domain **www[.]coronavirusapp.site** is still active but does not contain the malicious app download anymore. On March 17, 2020, it changed its appearance but still was hosting the same malicious file.
- It is **successfully blocked by Allot´s Network-based solution**

3.1 What Allot Blocked

This is the most common type of threat and the easiest to detect. There are multiple examples of websites disguised as Coronavirus “trackers”. For example, Allot started blocking thousands of incidents of Coronavirus.app per day starting on 26 March, 2020. Also detected and blocked were Coronavirus-monitor.ru and Covid19info.

4 Phishing using Coronavirus as bait

A more common method used by cybercriminals is **Phishing.** With this technique, the cybercriminal spreads malicious websites usually via e-mail, most recently **supplanting the identity of the Center for Disease Control and Prevention (CDC).**

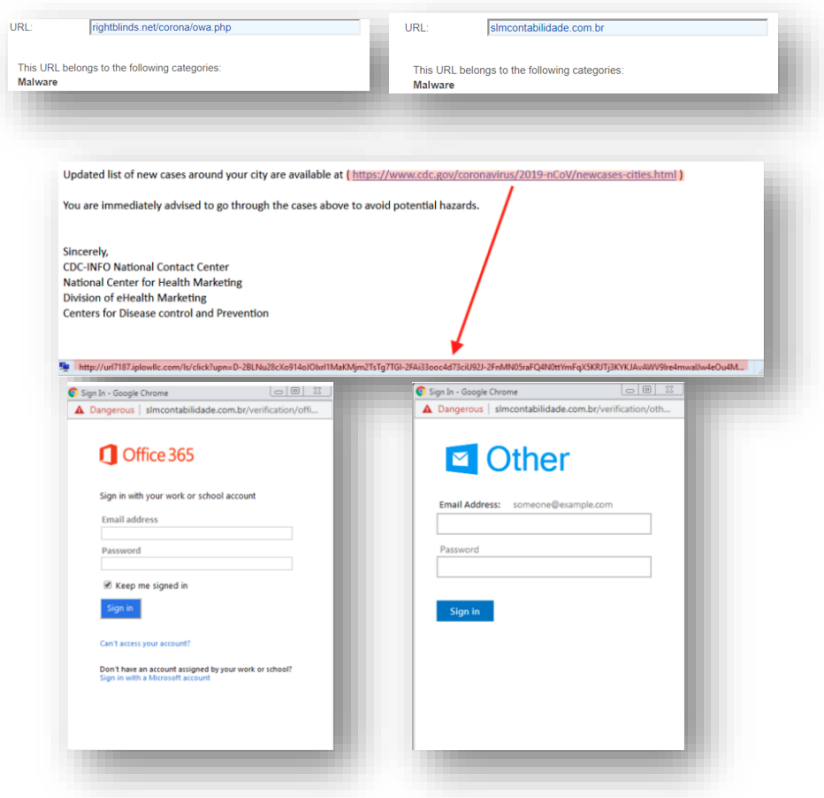
It uses two ways to make the victim visit the infected website:

1. Attached file (.word, .pdf) that opens a website when opening, or
2. A link in the text of the e-mail, disguised as a hyperlink to a legitimate website. (See the image on the right.)

There are two domains related to this method, one for each different way to trick the victim:

- hxxp:/rightblinds[.]net/corona/owa[.]php
- hxxp://slmcontabilidade[.]com[.]br

These links redirect the victim to an office 365 page that asks the victim to introduce their credentials. Fortunately, these malicious URLs are **successfully blocked** by our solution.



4.1 What Allot blocked

Allot started blocking Safefromcovid-19 starting on 26 March 2020. This attack let to a website “selling” face masks with significant discounts but in reality, it steals the bank details from the buyers.

5 Emails containing malware hidden in documents

Last but not least, it is commonly observed that cybercriminals are attaching **malicious documents inside e-mails** in order to trick users into clicking on malicious files.

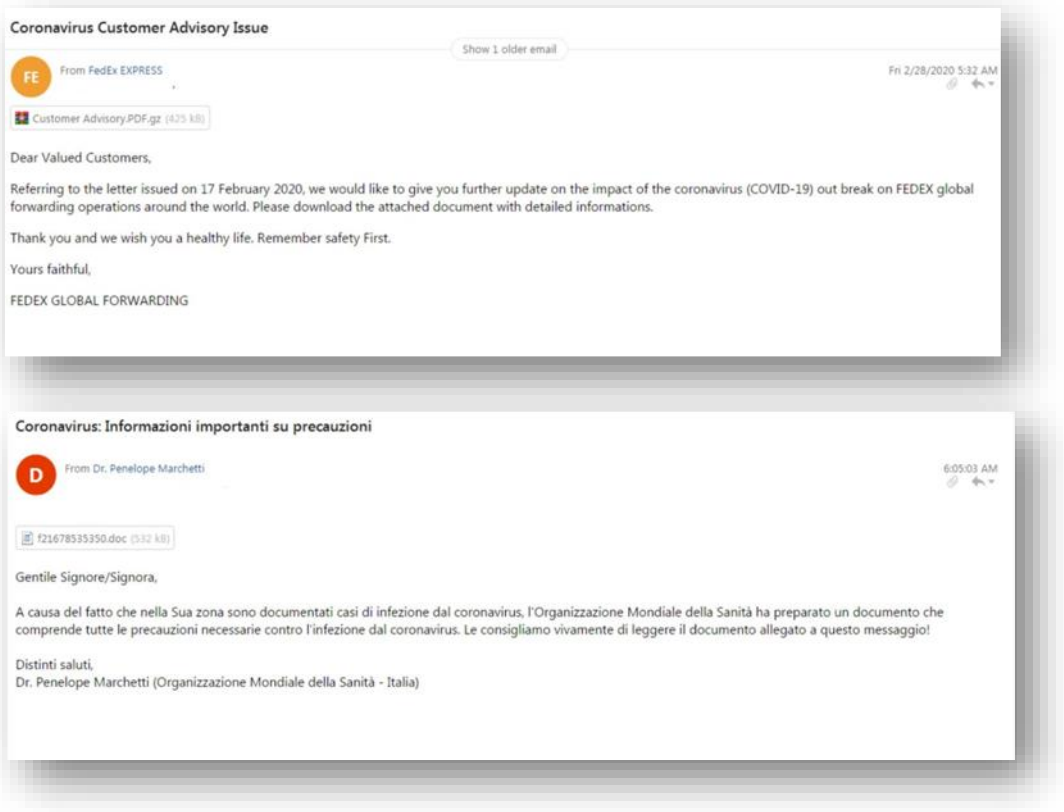
The cybercriminals disguise themselves as reliable sources such as **Ministries of Health, Centers for Public Health, or important national figures.**

To create the "feeling of urgency" in the victim, the e-mail states that the attached file contains critical information about coronavirus. Due to this feeling, the customer is more vulnerable to potential cyberthreats.

Two of the threats that are using this method as a method of infection are:

- **Trickbot**
- **Lokibot**

The signature of the virus is successfully detected and blocked by our antivirus e-mail solution.



6 Conclusions and Advice

The **Coronavirus crisis is a "hard-to-live-with" situation but we cannot allow ourselves to lower our guard against cyberthreats.** Cybercriminals will not stop their malicious actions. So, we cannot stop our precautions. Please follow these **recommendations** and transmit them to your end customers:

- Always verify the e-mail source
- Do not open files attached from an untrusted sources
- Before clicking on any hyperlink, verify where it redirects
- Do not send important information via e-mail (there are multiple sources where you can check if the information is true).
- In these dangerous times, it is important to be protected by a reliable security solution that protects you both from malicious URLs and infected files – We are proud at Allot to be your partner offering such protection.

7 Is that all?

NO. Definitely not**.** Above are the most significant URLs we are protecting against over the last days, but **this battle has just begun. In the coming days and weeks we will surely see more cyberthreats related to Coronavirus.**

This is something to have in mind. There are threats **everywhere,** But we only see the tip of the iceberg in online news and TV. There are many unknown **dangers** waiting for incautious victims to fall into their trap.

In a single 24-hour period (19 March, 2020), **321 new URLs related to coronavirus** were added to our Allot platform coming **only from one of our multiple feeds**.

```
317  stpl.ca/covid/who/files/fcfceb6c8e80ba350e7476a688dfef03.php?e=luke.vanboeck
318  stpl.ca/covid/who/files/fd0f27a91372d829f6d2ab17cfbedc3f.php    malware-lg
319  stpl.ca/covid/who/files/fd775901f72e2e39681b8a9ba2eedd77.php    malware-lg
320  track.frmp.it/y.z?l=http://www.metroparks.org/covid-19&j=333314953&e=3509&p=
321  zep0de.com/covid-19.zip malware-lx
```

At **Allot, we will continue to work to keep our protection systems updated** in order to provide peace of mind to your final customers.

For more on how to protect your at-home subscribers, watch the Allot webinar: *"It's a New Reality: Cybersecure Your Customers at Home"*.

www.allot.com sales@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA - Tel: +1 781-939-9300; Fax: +1 781-939-9393; Toll free: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 Sophia Antipolis, Cedex France - Tel: +33 (0) 4-93-001160; Fax: +33 (0) 4-93-001165
Asia Pacific: 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104, Tel: +65 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626

allot
See. Control. Secure.