This global health crisis continues to cause major impact to business, markets and economy. As seen over time, global events such as this automatically translates to a series of online exploitations by the cybercriminals.

As the virus intensifies in volume and scope, so does the wave of threat attacks and campaigns that use it as bait.

Trend Micro Research monitors this attack and this brief summary summarizes all our findings. This will be updated regularly as new threats are discovered and critical updates are released.
Map of threats using COVID-19

This data reflects findings from January 1 to March 31, 2020
COVID-19-Related Threats in Q1 2020

- 907K Total spam messages related to COVID-19
- 737 Detected malware related to COVID-19
- 48K Hits on malicious URLs related to COVID-19
- 220x Increase in spam from Feb. to Mar. 2020
- 260% Increase in malicious URL hits from Feb. to Mar. 2020

United States
Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period: January 1st to March 31st, 2020).*
Top countries with users accessing malicious COVID-related URLs

- United States: 15.0%
- Japan: 13.8%
- Germany: 9.8%
- France: 8.1%
- Taiwan: 6.2%
- United Kingdom: 5.3%
- Venezuela: 5.1%
- Indonesia: 4.3%
- India: 2.7%
- Australia: 2.6%
- Others: 27.1%

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020.
Instances that malicious COVID-19 related URLs were accessed

March 34,197
February 9,497
January 3,916

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution. This data reflects findings from January 1 to March 31, 2020.
Monthly spam email detections
(containing covid, covid-19, coronavirus, or ncov)

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020.
Monthly detections for malware related to COVID-19
(with covid, covid-19, coronavirus, or ncov in the filename)

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.
This data reflects findings from January 1 to March 31, 2020.
Emotet was discovered 2014 from a known as a banking malware variant that stole data by sniffing out network activity evolved more complex form acting as a loader for other malware families.
SPAM: top method to deliver attacks on enterprises

94.9%

Top 2 Spam Samples

- Shipment Notification
- Coronavirus Ministry of Health Updates
Expected growth in EMAIL SCAM proliferation

Top Emerging Techniques

1. Targeting specific countries, including China and Italy
2. Business Email Compromise
3. Cruel ransomware
4. Sextortion-related scams

Good morning Paul,

How are you? I hope that everything is okay.

Following the dramatic situation in Europe and in many countries, I am personally managing a financial operation in collaboration with the Valther Avocats in France.

Mr. Theron is representing them.

I will need you to assist him, and give him the necessary support on the subject.

It is important to manage this file ASAP because we are already late due to the corona situation...

This file is confidential for the moment, I count on your absolute discretion.

Mr. Theron was supposed to contact you this morning, has it been done?

Kind regards,

BEC email

Coronavirus extortion email spam

Targeting specific countries, including China and Italy

Business Email Compromise

Cruel ransomware

Sextortion-related scams
INFO-THEFT THROUGH CORONAVIRUS INTERACTIVE MAP

An interactive coronavirus map was used to spread information-stealing malware.

MALICIOUS MOBILE APPLICATION

A mobile ransomware named CovidLock comes from a malicious Android app that supposedly helps track cases of COVID-19.

Threat actors exploit the public’s need for information about Covid-19 to distribute malware.
Threat actors exploit the public’s need for information about Covid-19 to distribute malware.

**FAKE COVID-19 SAFETY PORTAL FROM THE WORLD HEALTH ORGANIZATION (WHO)**

Phishing site that pretends to be a WHO portal.

**FAKE CENTER FOR DISEASE AND PREVENTION WAITLIST**

Another phishing site aiming to get personal information.
The coronavirus’ effects have reached the CYBERCRIMINAL UNDERGROUND

Popular Items Now Sold in the Underground

- Covid-themed phishing, malware, and exploits
- Toilet paper, N95 masks, ventilators, and other essential supplies
Trend Micro endpoint solutions such as the Smart Protection Suites and Worry-Free™ Business Security detect and block the malware and the malicious domains it connects to.

As an added layer of defense, Trend Micro™ Email Security thwarts spam and other email attacks. The protection it provides is constantly updated, ensuring that the system is safeguarded from both old and new attacks involving spam, BEC, and ransomware.


A multilayered protection is also recommended for protecting all fronts and preventing users from accessing malicious domains that could deliver malware.
Developing Story: Coronavirus Used in Malicious Campaigns

March 26, 2020


The coronavirus disease (COVID-19) is being used in a variety of malicious campaigns including spam, malware, ransomware, and malicious domains. As the number of those afflicted continues to surge by thousands, campaigns that use the disease as a lure increase.

Related Posts:
- Working From Home? Here’s What You Need for a Secure Setup
- Malware Ransomware Threats to Exposure Stolen Data
- New Variant of Paradise
- Darknet ransomware Spreads Through SD Card
- New Variant of Paradise

2020 PREDICTIONS: “Home offices will redefine supply chain attacks”

WORKING FROM HOME GUIDE

Fundamental security practices and guidance for employees/organizations and consumer/families how conduct business safely online