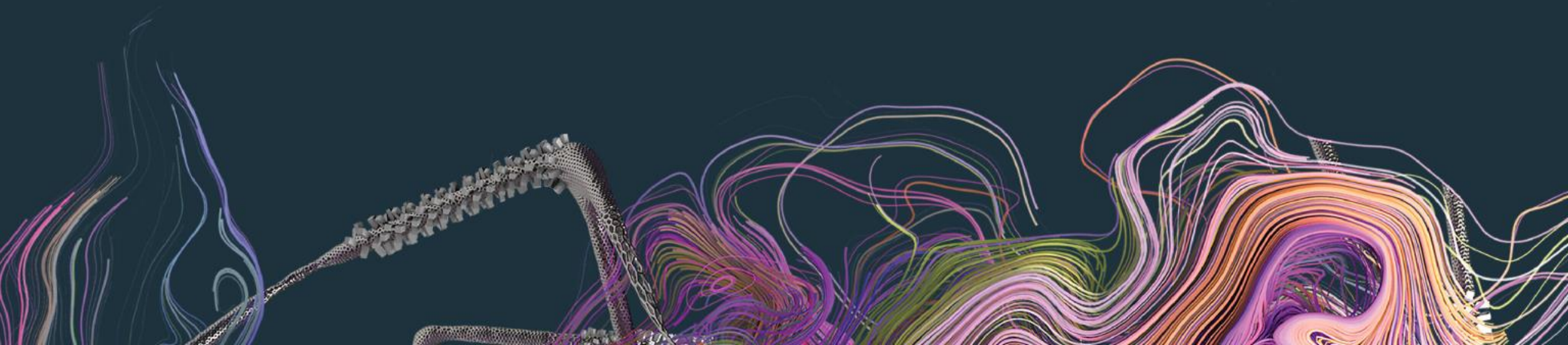
TREND MICRO™ | research



CORONAVIRUS-RELATED THREATS

BRIEF SUMMARY as of April 13

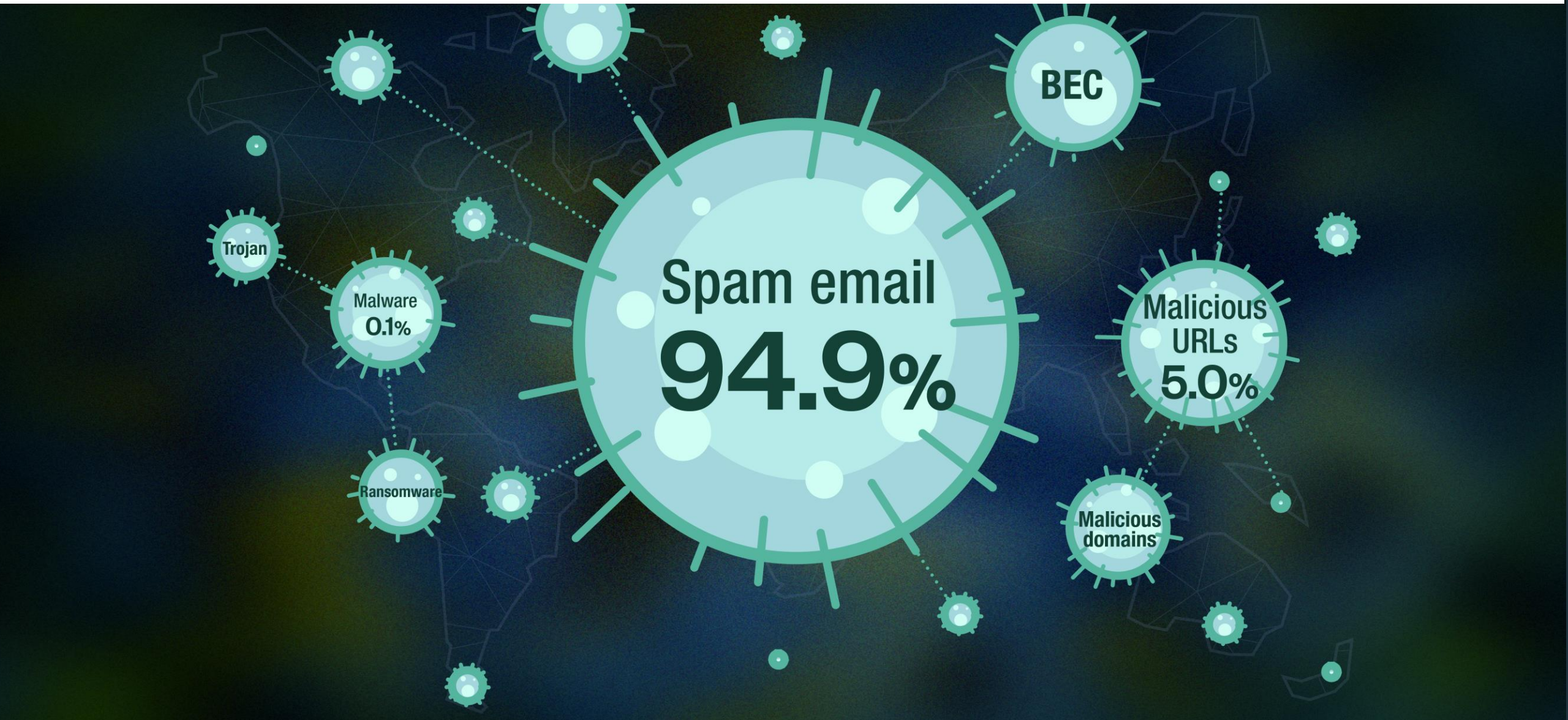
This global health crisis continues to cause major impact to business, markets and economy. As seen over time, global events such this automatically translates to a series of online exploitations by the cybercriminals.

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.

TREND MICRO | research

Map of threats using COVID-19



This data reflects findings from January 1 to March 31, 2020

©2020 TREND MICRO

BY THE NUMBERS

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 1 to March 31 2020).

TREND MICRO | research

Photo by Fusion Medical Animation on Unsplash

© 2020 Trend Micro Inc.

Top countries with users accessing malicious COVID-related URLs

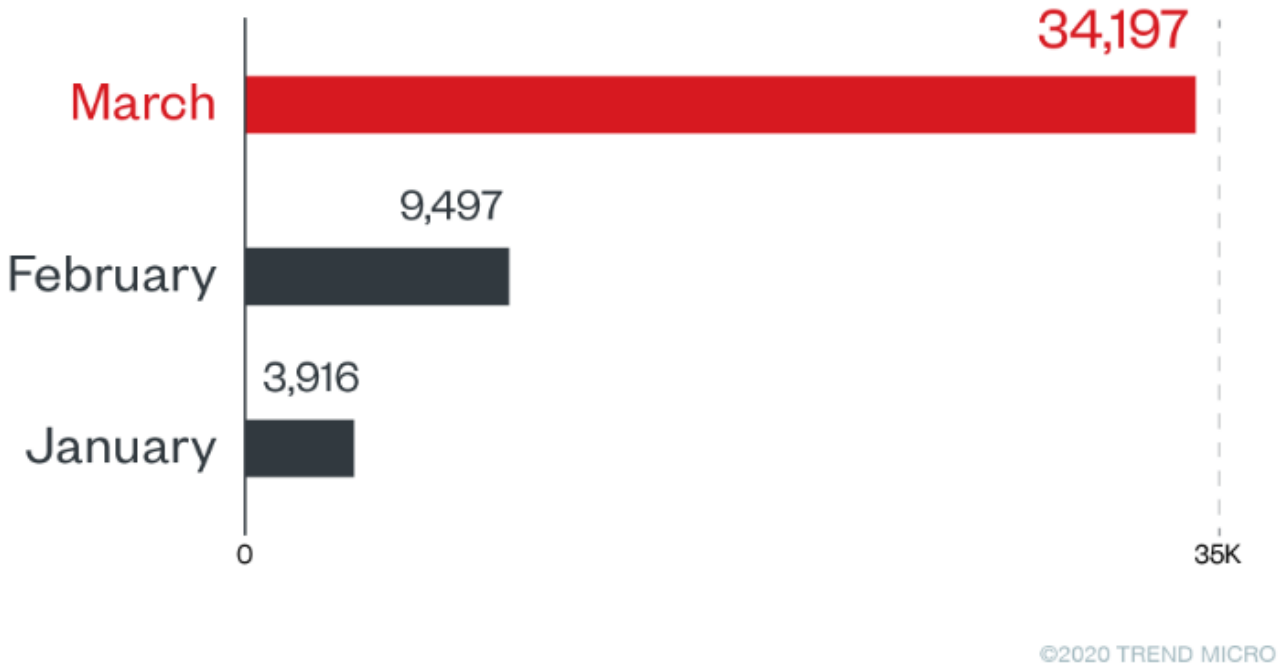
United States	15.0%
Japan	13.8%
Germany	9.8%
France	8.1%
Taiwan	6.2%
United Kingdom	5.3%
Venezuela	5.1%
Indonesia	4.3%
India	2.7%
Australia	2.6%
Others	27.1%

©2020 TREND MICRO

*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

© 2020 Trend Micro Inc.



Instances that malicious COVID-19 related URLs were accessed

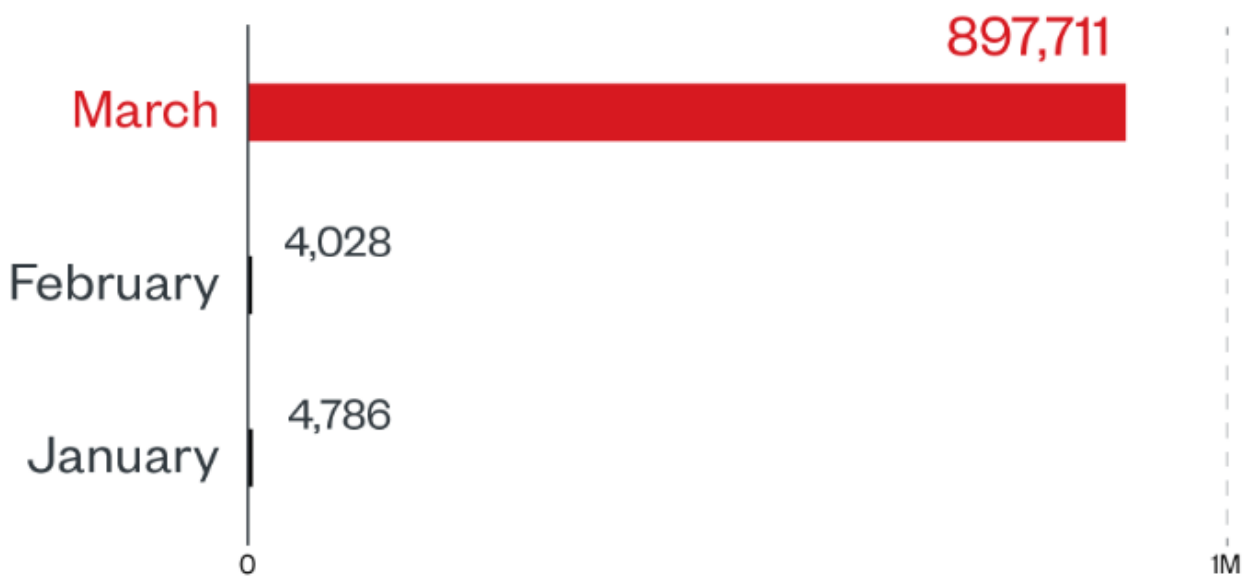
*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020

© 2020 Trend Micro Inc.

Monthly spam email detections

(containing *covid*, *covid-19*, *coronavirus*, or *ncov*)



©2020 TREND MICRO

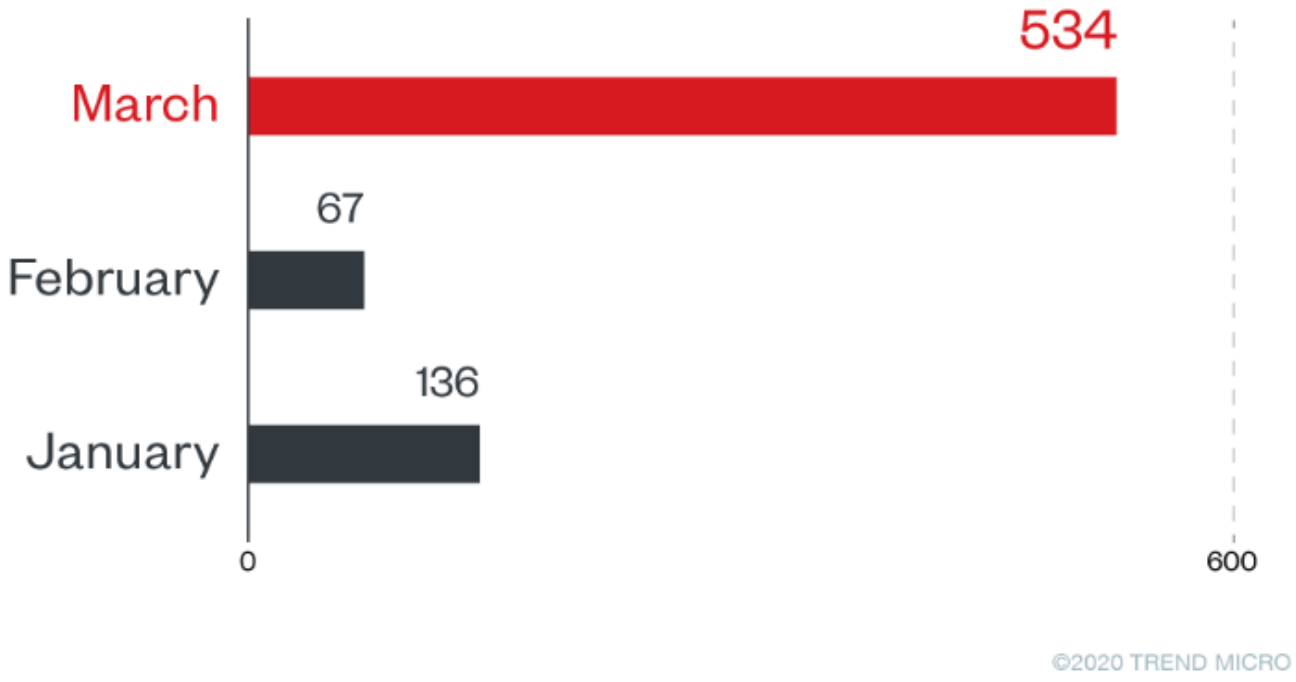
*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020

© 2020 Trend Micro Inc.

Monthly detections for malware related to COVID-19

(with *covid*, *covid-19*, *coronavirus*, or *ncov* in the filename)

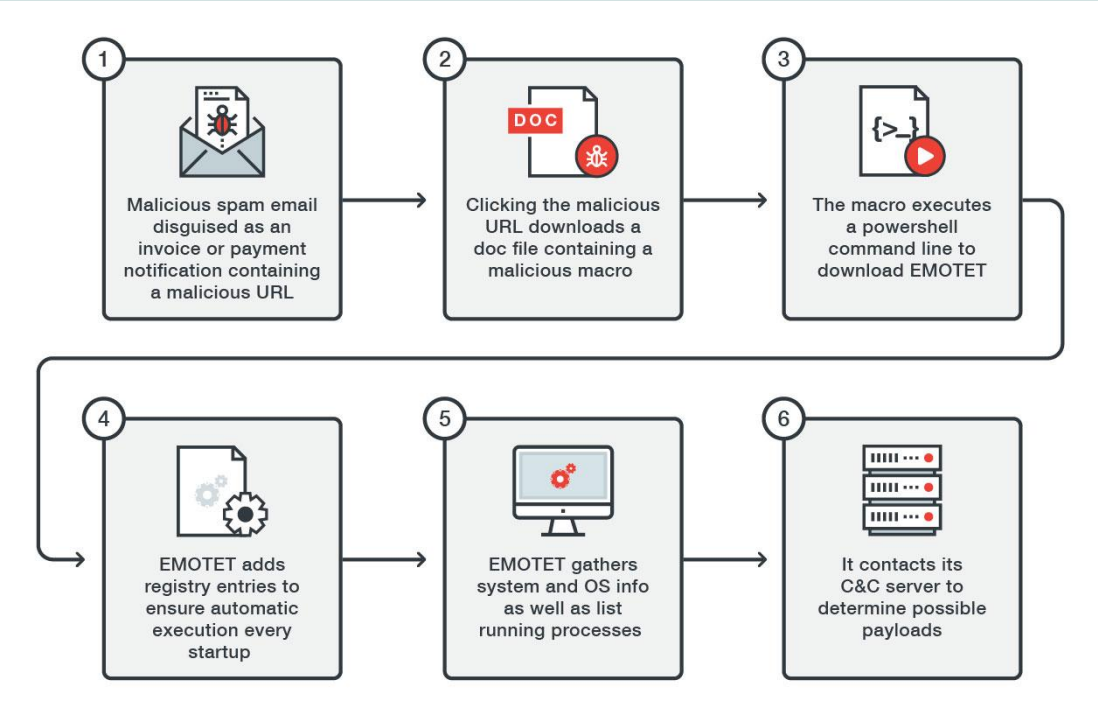


*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020

© 2020 Trend Micro Inc.

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



EMOTET Infection Diagram for the recent wave of attacks

EMOTET

was prominently used in coronavirus campaigns

© 2020 Trend Micro Inc.

Re: Cancel shipment due to corona virus _ New Shipping schedule details - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

Reply Reply All Forward More

From [redacted]

Subject **Re: Cancel shipment due to corona virus _ New Shipping schedule details** 02/11/2020, 9:13 PM

To [redacted]

Dear

We are planning to ship the following orders next week but due to the corona virus we have postponed below shipment.
Please check details attached new shipping info and the shipping instructions and advice if we should still proceed

If you are no problem with above shipment time, we will proceed the shipment.

Thanks & Best Regards,

****

Tokyo tinplate sales department Trade team

Export Ando Import Dept.

Save

Corona Virus Latest Updates - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

Reply Reply All Forward More

From Ministry of Health News Portal [redacted]

Subject **Corona Virus Latest Updates** 02/07/2020, 3:34 AM

To [redacted]

Good day,

Given the changing dynamics of the outbreak in China and globally, and recognizing we are in the midst of influenza season, we ask anyone who has been in China especially in Hubei province to consider staying home and keeping their children home until 14 days have passed from their last visit to Hubei.

Monitor yourself, relative and your children closely for symptoms, and if any symptoms arise, connect with your primary care provider, local public health office or call 811. This is an important way to reduce the possibility of transmission of illness to others.

We remain in regular contact with Chinese government and the province and are monitoring the situation closely, and will continue to keep you informed of new developments.

Kindly view and share the attached for latest updates and advice from the province, while we will continue to keep you informed of new developments.

Please note, if you are unsure of the origin of an external email please exercise caution before clicking on links or opening attachments.

1 attachment: Coronavirus Latest update.dat 32.4 KB

Save

SPAM: top method to deliver attacks on enterprises

94.9%

Top 2 Spam Samples

- Shipment Notification
- Coronavirus Ministry of Health Updates

TREND MICRO

From:
Date: March 26, 2020 at 1:06:42 PM GMT+8
To: "[redacted]"
Subject: I can infect you with COVID-19

I know everything little secret about your life.
To prove my point, that is why i am sending you this email from your system using your email account.

I am aware of your whereabouts, what you eat, with whom you talk to, every little thing you do everyday.

What am i capable of doing?
If i want, i could infect You and your whole family with the Corona Virus **(COVID-19).**
Reveal all your secretes, There are countless things i can do.

What should you do?
transfer the amount of **$500** to my bitcoin address (if you do not know how to do this, write to Google: "Buy Bitcoin" or https://www.coinmama.com).

My bitcoin address (BTC Wallet) is: 1HEGxH9pZwYCnxf2PQCvyKzB2JzairA82W

After receiving the payment, you will never hear me again.

I give you 72 hours (NOT more than 3 days) to pay, failure to do this, I will infect YOU and every member of your family with the Corona Virus **(COVID-19).**
no matter how smart you are, and believe me, i will completely ruin your life.

I have a notification reading this letter, and the timer will start to work when you see this letter.
Don't waste your time replying this email because it was sent from your system and email account.

If I find out that you have shared this message with someone else or try to report this, Then YOU and every member of your family will be infected with the Corona Virus **(COVID-19).**

Coronavirus extortion email spam

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 suppose to contact you this morning, has it been done ?

Kind regards,

BEC email

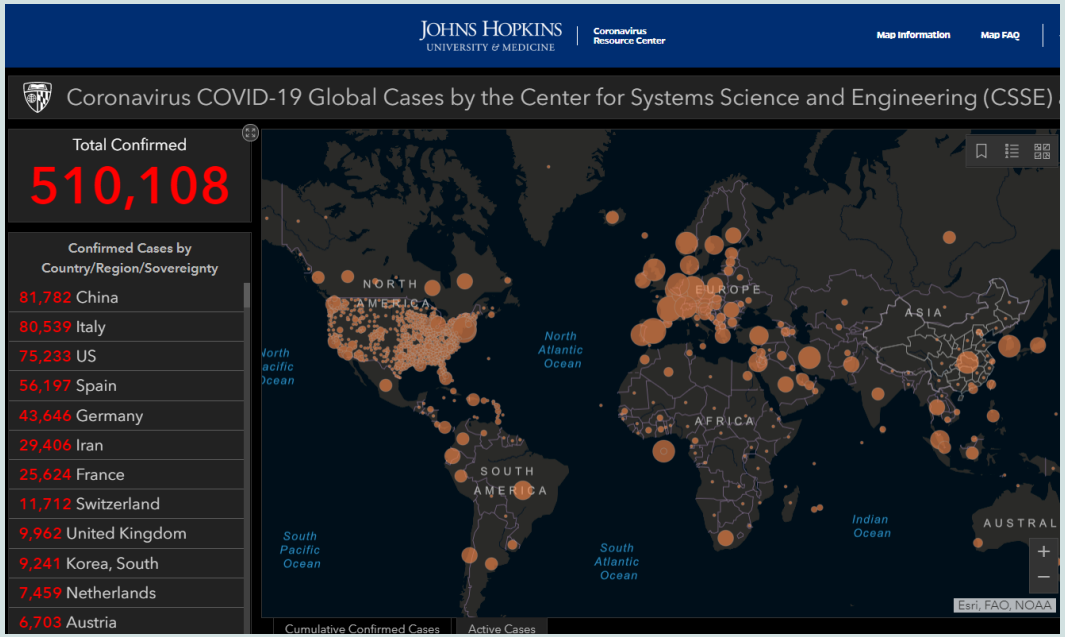
Expected growth in **EMAIL SCAM** proliferation

Top Emerging Techniques

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

© 2020 Trend Micro Inc.

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



INFO-THEFT THROUGH CORONAVIRUS INTERACTIVE MAP

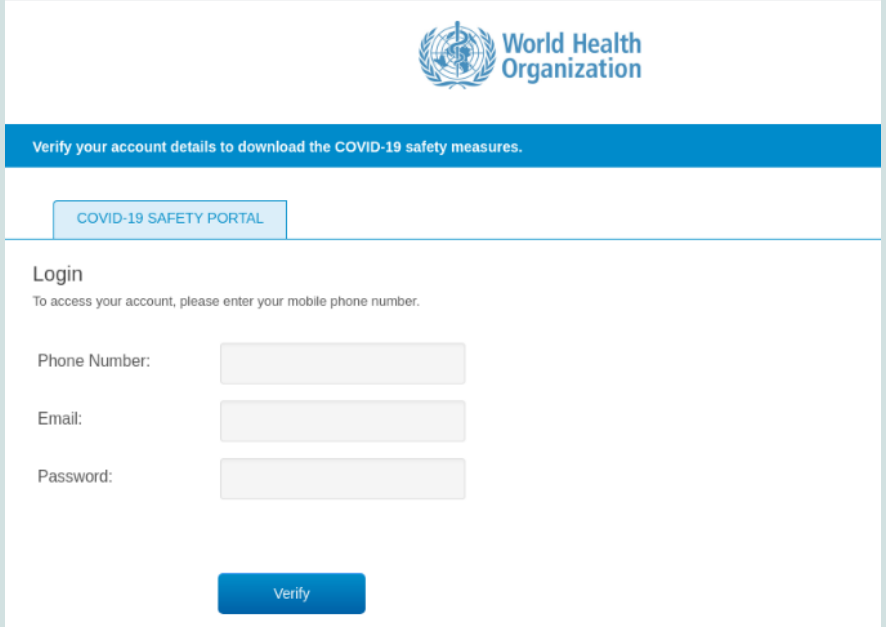
An interactive coronavirus map was used to spread information-stealing malware.

MALICIOUS MOBILE APPLICATION

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

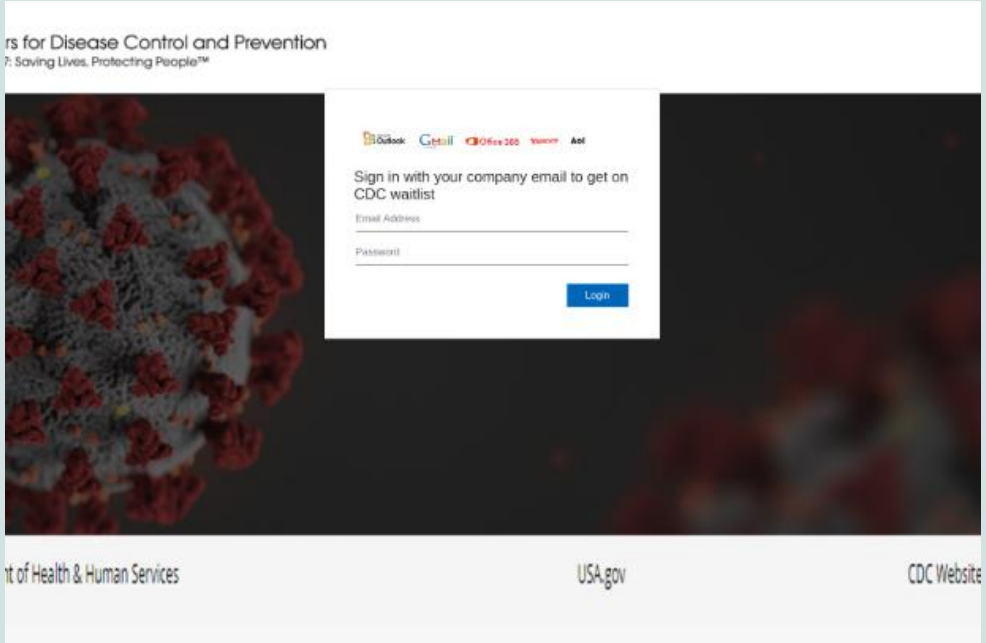
© 2020 Trend Micro Inc.

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.

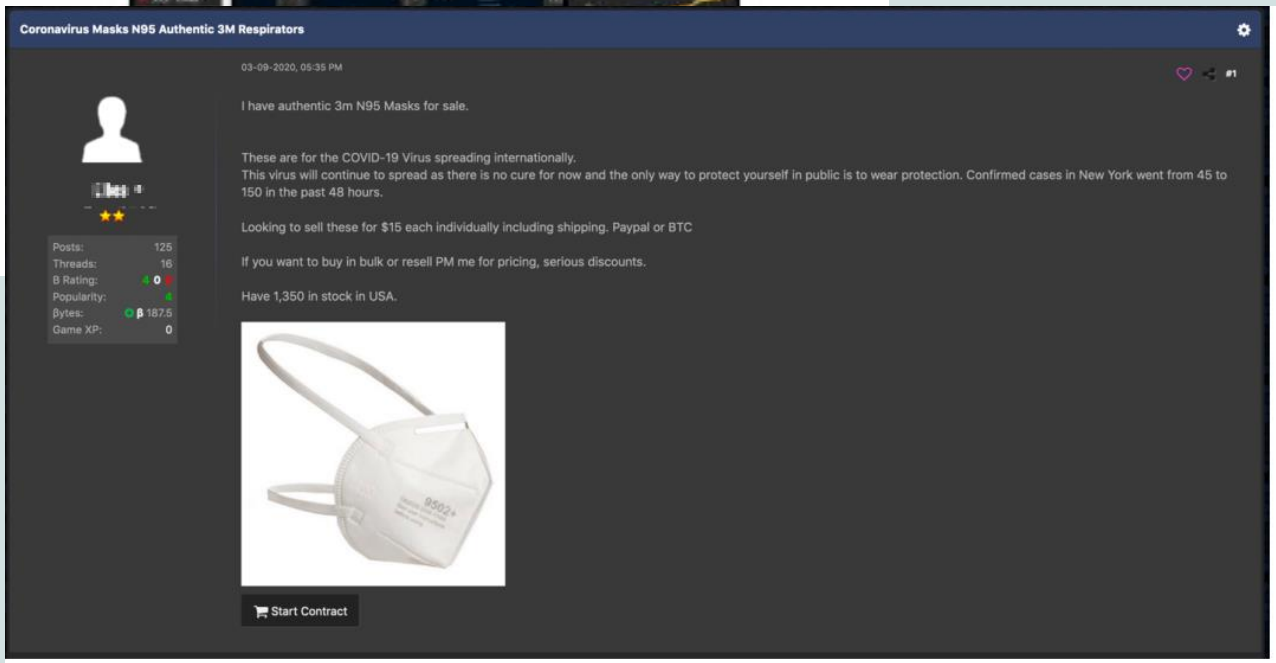


FAKE CENTER FOR DISEASE AND PREVENTION WAITLIST

Another phishing site aiming to get personal information.

© 2020 Trend Micro Inc.

Coronavirus-themed phishing exploit sold on underground forum



Forum post offering N95 masks

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

© 2020 Trend Micro Inc.

DEFENSE AGAINST THESE THREATS

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.

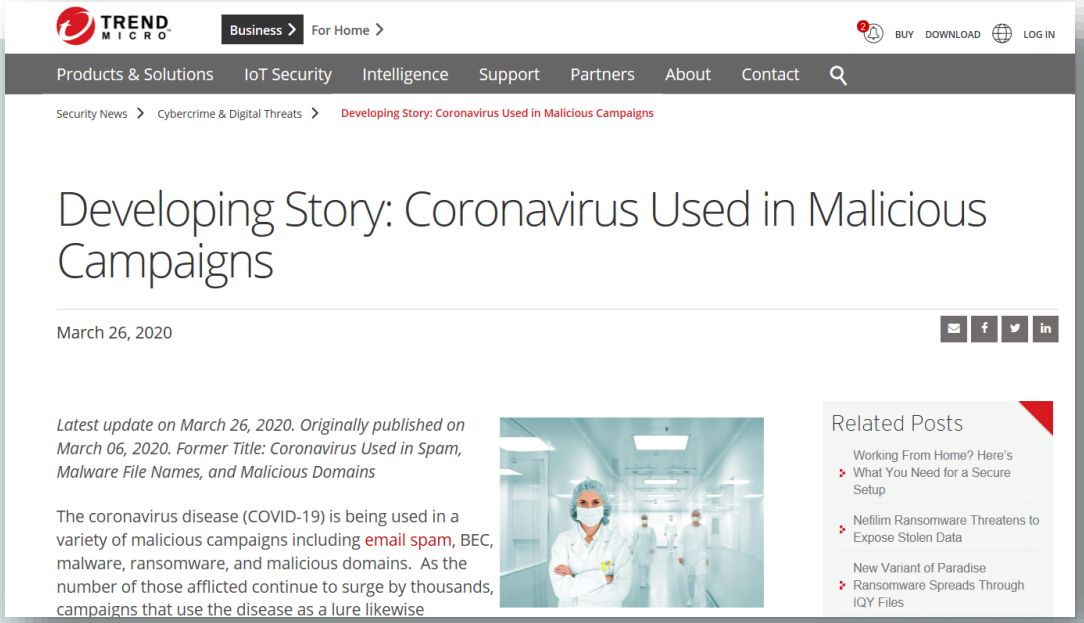
As an added layer of defense, **Trend Micro™ Email Security** thwarts spam and other email attacks. The protection it provides is constantly updated, ensuring that the system is safeguarded from both old and new attacks involving spam, BEC, and ransomware.

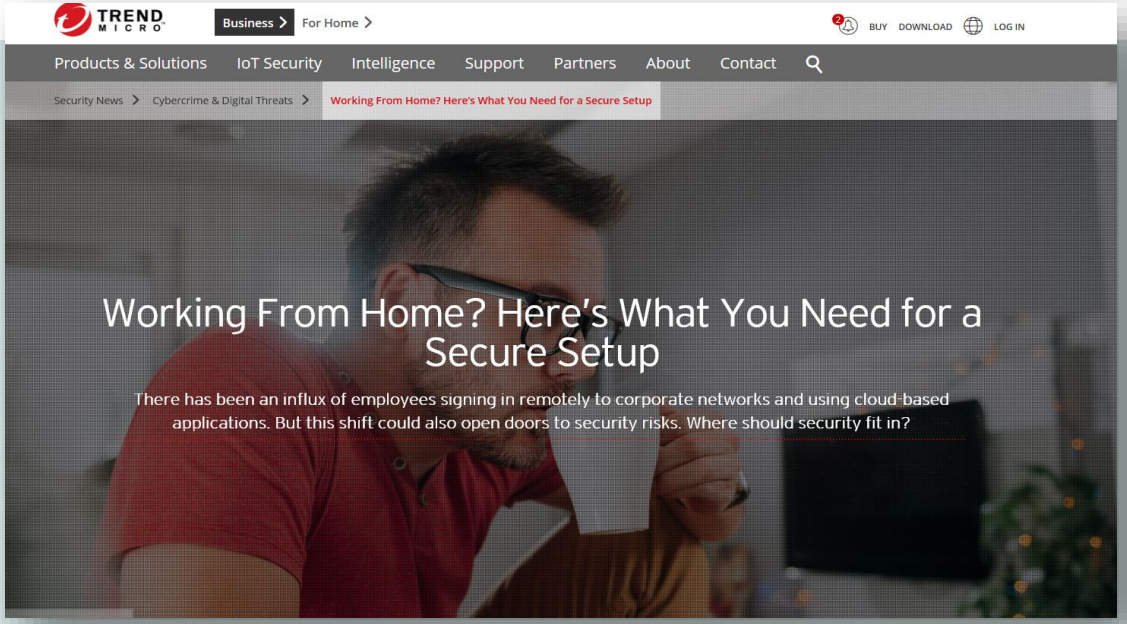
Trend Micro's Cloud App Security finds unknown malware using machine learning. The document exploit detection engine uncovers threats hidden in office files while artifical intelligence checks email behaviour, intention, and authorship to identify BEC attacks.

A **multilayered protection** is also recommended for protecting all fronts and preventing users from accessing malicious domains that could deliver malware.

© 2020 Trend Micro Inc.

GET MORE INFORMATION





2020 PREDICTIONS: *"Home offices will redefine supply chain attacks"*

DEVELOPING STORY : CORONAVIRUS Threats and Campaigns

Official landing page for all threat and security findings related to this virus

WORKING FROM HOME GUIDE

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

© 2020 Trend Micro Inc.

TREND MICRO | research

TWITTER

https://twitter.com/TrendMicroRSRCH

BLOG

https://blog.trendmicro.com/trendlabs-security-intelligence/

SECURITY NEWS

https://www.trendmicro.com/vinfo/us/security/news/