5 Times More Coronavirus-themed Malware Reports during March

Anti-Malware Research

5 min read

Liviu ARSENE

March 20, 2020

Government, Hospitality, Healthcare, Education & Research, and Retail are among the verticals most targeted on the Coronavirus heatmap.

As the Coronavirus pandemic continues, cybercriminals have started piggybacking news of the crisis to deliver malware, conduct phishing, and even perform online fraud by preying on the panic caused by a dearth of medical supplies and reliable information about the pandemic.

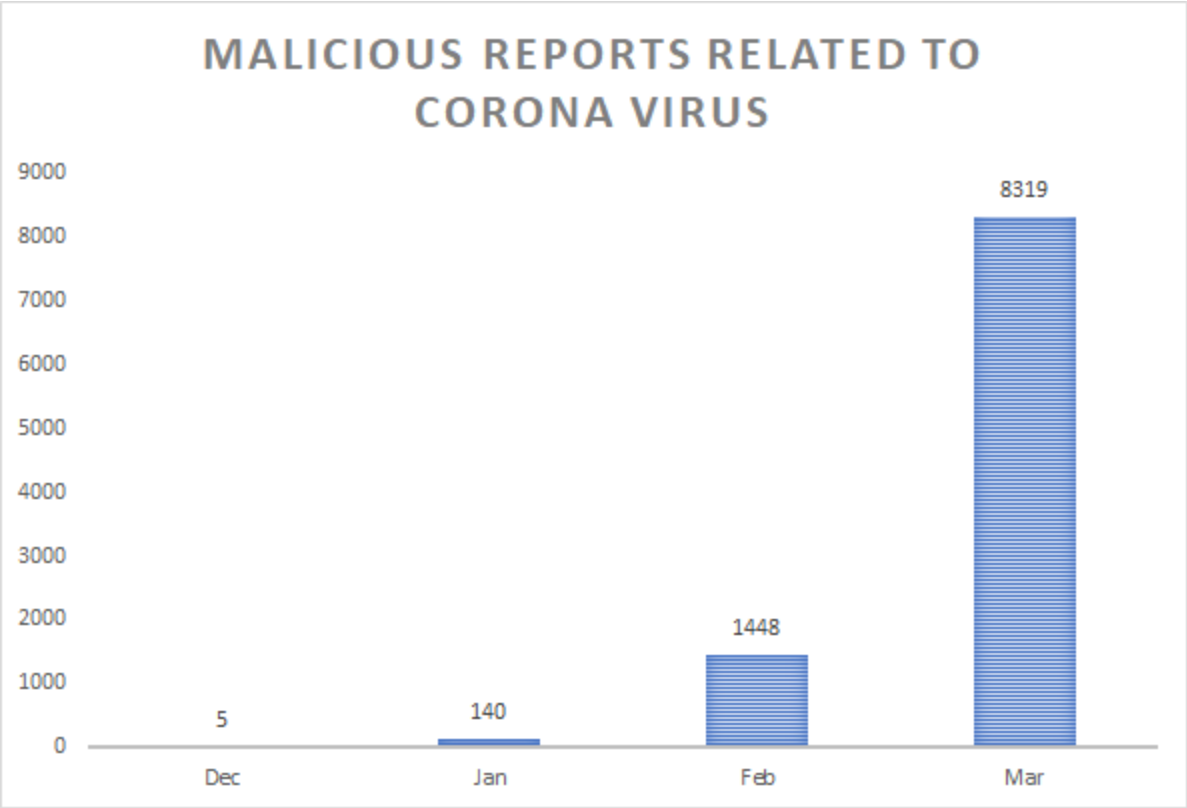
The most recent Bitdefender telemetry shows unusual activity regarding Coronavirus-related threats: the number of malicious reports related to Coronavirus has increased by more than 475% in March, compared to February. And we still have about two more weeks to go until April.

These campaigns were likely mostly targeted at countries that have started suffering an increase in Coronavirus infections, leveraging the fear on everyone's mind.

With officials struggling to come up with plans and quarantine procedures, threat actors seem to have mobilized quickly and started luring victims with the promise of new and exclusive information on protection procedures.

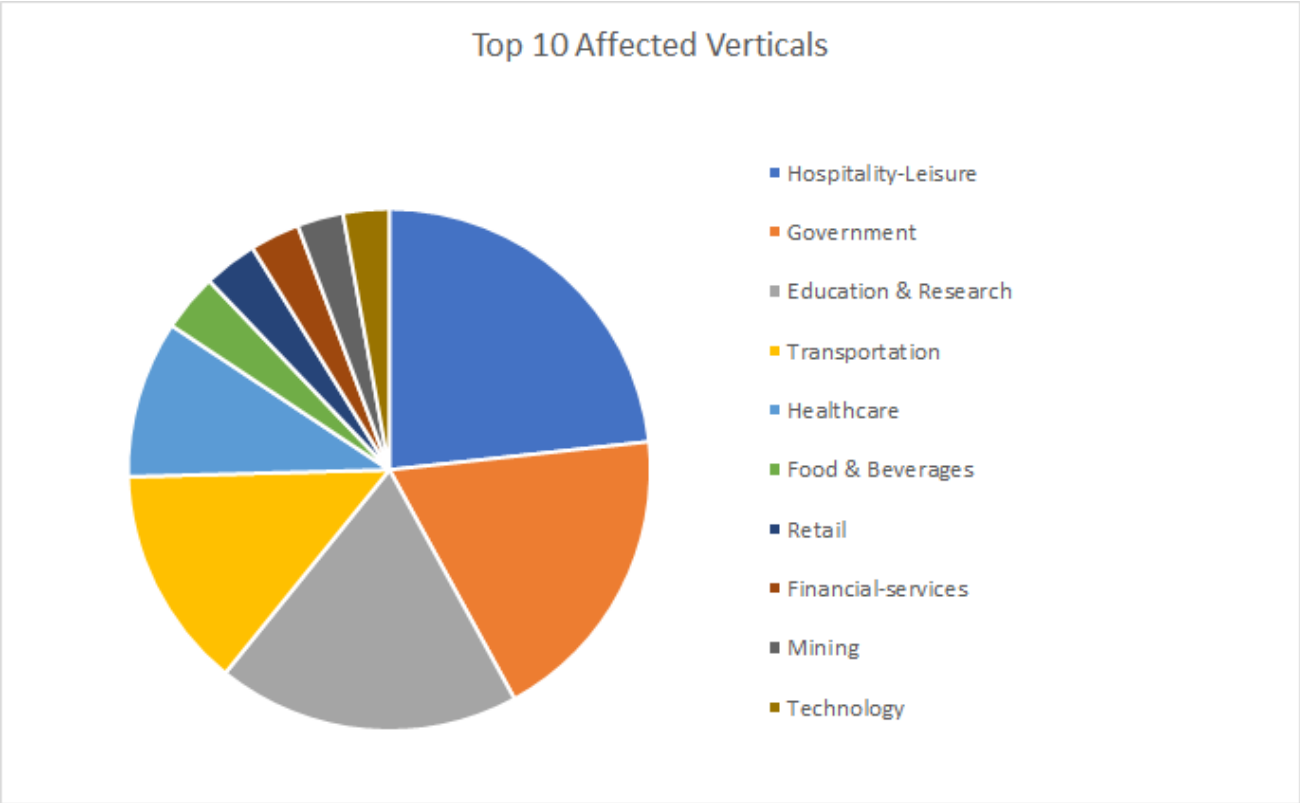
Malicious Reports Soar in March

From 1,448 malicious reports in February to 8,319 reports until March 16th, the number has sharply increased, as the real COVID-19 virus spreads aggressively around the world.



Some of the most-targeted verticals seem to be government, retail, hospitality, transportation and education & research. While it may seem odd, it does make sense that these verticals are targeted as they actively interact with large groups of individuals and are most interested in learning more about measures to be taken to prevent a Coronavirus infection.

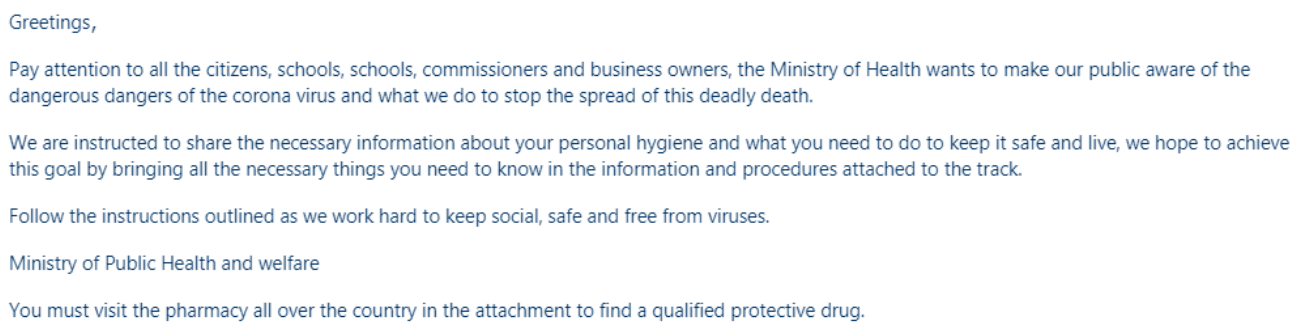
Consequently, one reason why cybercriminals have been actively targeting these verticals with phishing emails impersonating the WHO (World Health Organization), NATO, and even UNICEF is that employees likely expect official information from known, global organizations.



A breakdown into which Government institutions seem targeted most reveals that education ministries, health ministries and departments, and fire services have been attacked most.

In healthcare, hospitals & clinics, pharmaceutical institutions, and distributors of medical equipment, were mostly targeted, potentially with messages of procedures that need to be taken, drugs that could work on preventing or treating infection, and even medical supplies that were allegedly still in stock.

For example, the email above seems to target Healthcare services in Thailand judging from the title, which is translated from Thai ("Fwd: Re: CoronaVirus Express Information"), and the name of the attached file ("Ministry of Public Health Corona Virus Information Urgent 2020.gz"). It promises new and exclusive information to medical staff. To make the email seem more legitimate, it uses the official logos of the Thailand Establishment of National Institute of Health.


Greetings,

Pay attention to all the citizens, schools, schools, commissioners and business owners, the Ministry of Health wants to make our public aware of the dangerous dangers of the corona virus and what we do to stop the spread of this deadly death.

We are instructed to share the necessary information about your personal hygiene and what you need to do to keep it safe and live, we hope to achieve this goal by bringing all the necessary things you need to know in the information and procedures attached to the track.

Follow the instructions outlined as we work hard to keep social, safe and free from viruses.

Ministry of Public Health and welfare

You must visit the pharmacy all over the country in the attachment to find a qualified protective drug.

In rough translation, the email (seen above) urges citizens, schools, commissioners and business owners to follow the instructions in the attached document to stay "safe and free from the viruses." It also claims the file contains a list of pharmacies that distribute "a qualified protective drug." Needless to say, anyone opening the tainted attachment will be infected with a Trojan, specifically the NanoBot Trojan.

Education & Research verticals, where messages reached universities, schools, and technical institute, are all crowded places eagerly awaiting instructions on how to prepare for the Coronavirus outbreak. They too have been selectively targeted with spearphishing emails.

A look at some of the tainted documents received by government institutions shows all filenames, naturally, share the same "coronavirus" string and promise to offer new and exclusive information regarding the outbreak.

For example, popular document booby traps range from claiming the email attachments are PDF documents when in fact they're everything from ".exe" to ".bat" files. That means that, unless users have the "File name extensions" option ticked in the View menu of File Explorer; they'll likely fall for this double extension scam. Of course, the files are laced with malware and, as soon as they're executed, they start deploying threats ranging from LokiBot and HawkEye to Kodiac and NanoBot (see the table below).

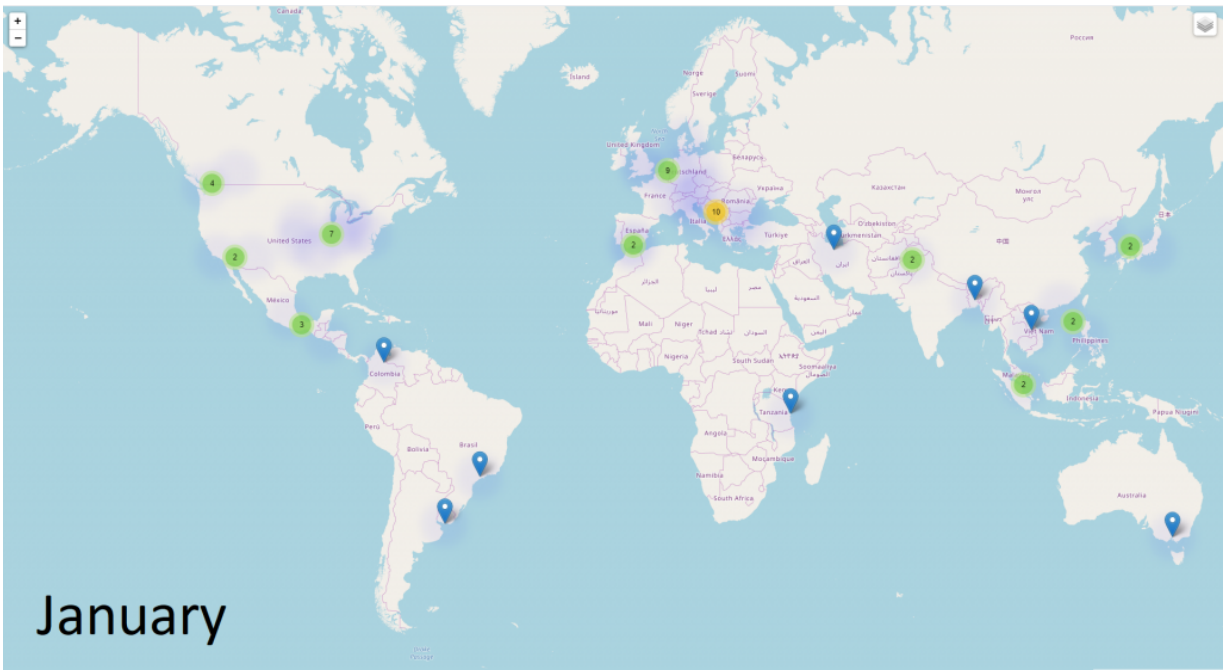
Most of these Trojans, including NanoBot, are designed to steal information, such as usernames and passwords, potentially for use by threat actors either for financial profit or to gain remote access to accounts, services, and even endpoints.

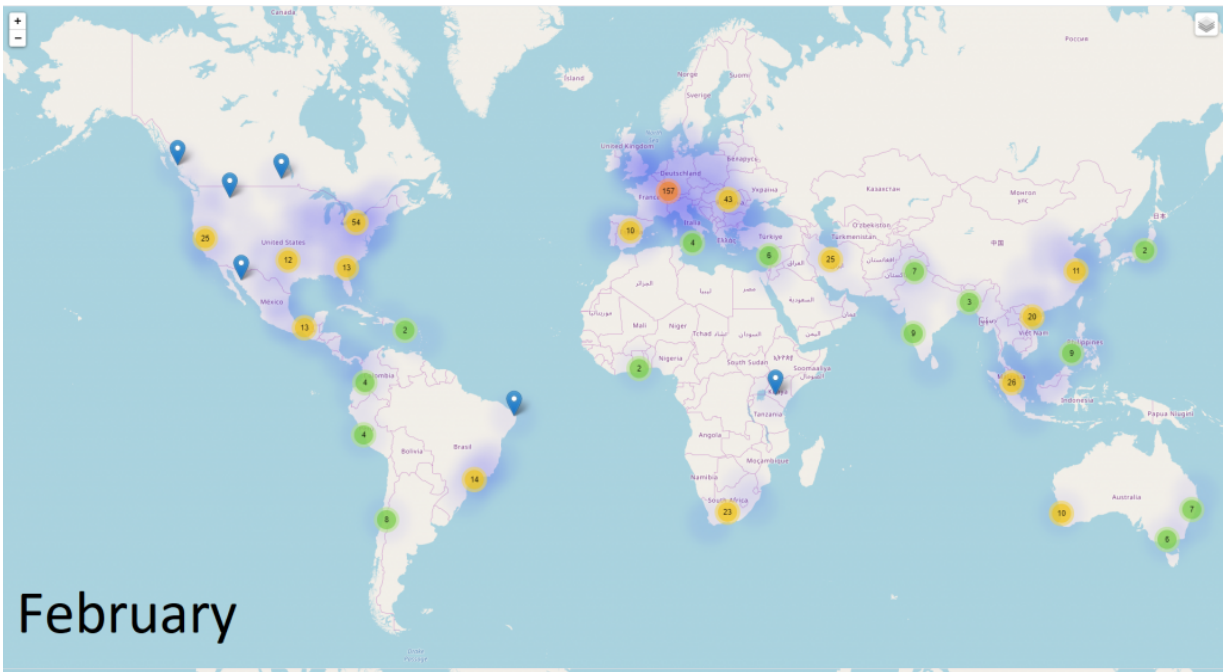
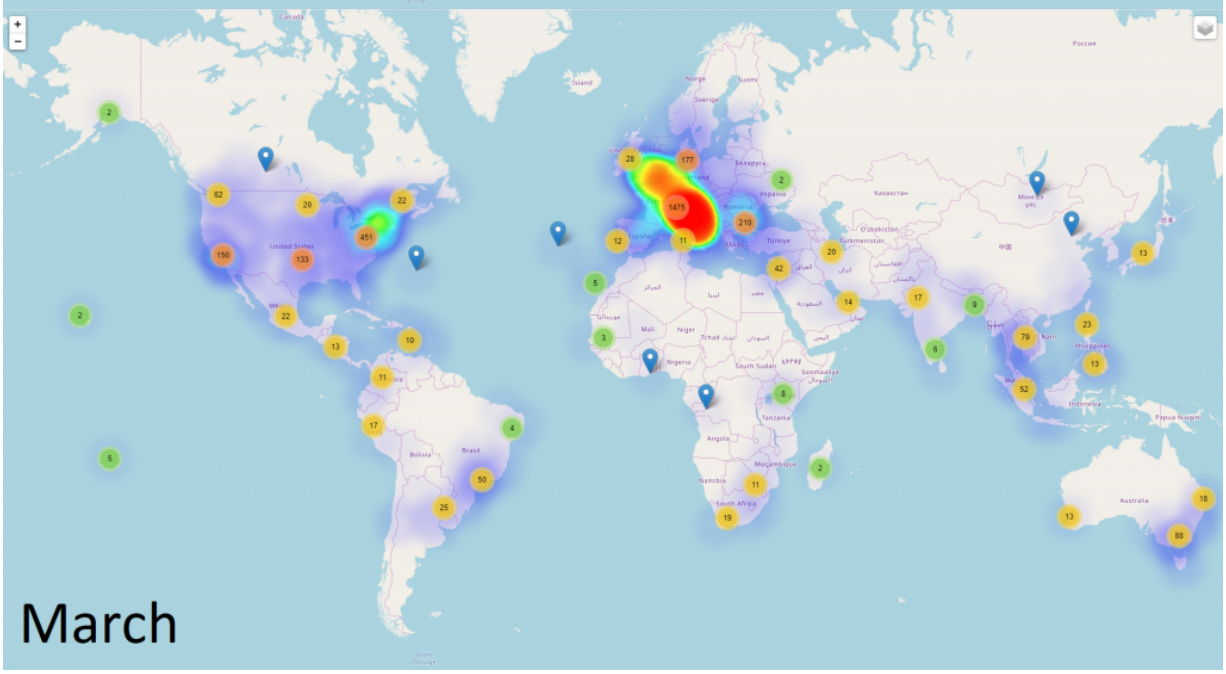
Below, you can see a table with examples of names for each malicious documents received by each vertical, along with each email subject (where applicable).

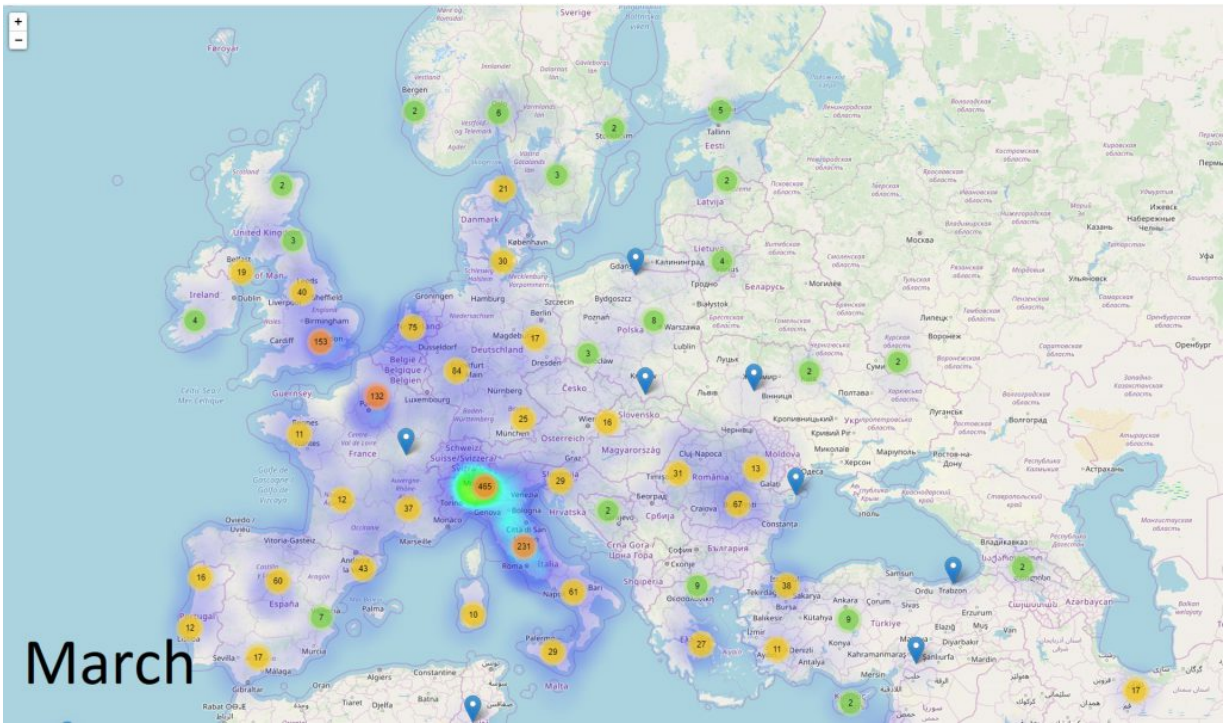
	Document Name	Email Subject Title	Detection
Government	covid19_bah.pdf.tar=>covid19_bah.pdf.exe	corona virus (covid-19 / 2019-ncov) impact to sea frei	LokiBot
Retail	world health organisation_pdf.gz=>world health organisation pdf.exe	w.h.o.coronavirus(cov) safety&preventive measures	HawkEye
	covid-19-list;contry ;product.xlsx	coronavirus finally struck america and european continent	Remcos
	indonesian health department_pdf.gz=>indonesian health department_pdf.exe	coronavirus di indonesia: tahu cara melindungi dan mencegah diri. jangan mendapat infeksi	GuLoader
Hospitality	recommendations coronavirus.doc=>recommendations after infection.pdf.bat	N/A	Koadic
	f18258643426.doc	coronavirus: informazioni importanti su precauzioni	Ostap
Healthcare	Ministry of Public Health Corona Virus Information Urgent 2020.gz	Fwd: Re: CoronaVirus Express Information	NanoBot

Going After Countries Aggressively Affected by COVID-19

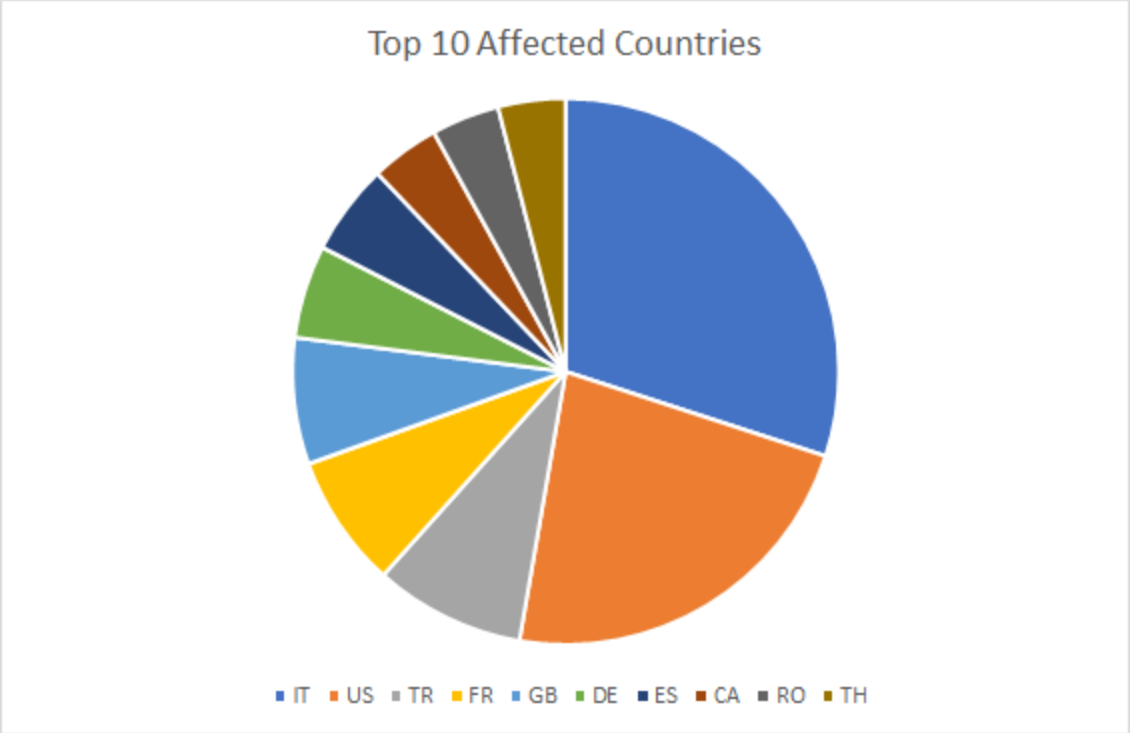
In terms of the geographical distribution for all malicious reports involving the Coronavirus, things escalated quickly between January and March. In January, reports were coming in only from some countries such as the United States, China, and Germany. By March, malicious reports came in from all around the world, and no European country was spared.

- 

- 
February
- 
March

- 

In fact, during March, the largest number of malicious reports was registered from countries such as Italy, the United States, Turkey, France, the United Kingdom, Germany, Spain, Canada, Romania, and Thailand. All these countries that have been seriously afflicted by the COVID-19 outbreak, which is why it's likely these malware campaigns have been focusing specifically on these regions.



As if having to deal with the Coronavirus in real life wasn't enough, threat actors have been exploiting panic, misinformation, and confusion in an attempt to maximize their efforts in spreading scams and infections or generally profiting off of everyone's fears.

Here’s what you should know

With countries straining to find ways to contain and even stop the spread of COVID-19 infections, the average user/citizen is undoubtedly seeking help and information from any online source on how to stay safe. However, that information may not always come from a reputable source.

Malware is a dime a dozen and cybercriminals will stop at nothing to trick users into installing it. It may already be difficult to cope with the real-life virus, and dealing with cyber “viruses” is probably the last thing on anyone’s mind.

However, just like in real life, good (security) hygiene means you’re not only keeping yourself safe but you’re also helping those around you. So carefully read through emails to make sure they’re legitimate, don’t open attachments unless you’re absolutely sure they’re safe, and try using a security solution that can keep you safe from a wide range of threats, so you can focus on what matters: keeping your family safe!

Note: This article is based on technical information provided courtesy of the Bitdefender Labs teams.

TAGS

anti-malware research

AUTHOR

Liviu ARSENE

Liviu Arsene is the proud owner of the secret to the fountain of never-ending energy. That's what's been helping him work his everything off as a passionate tech news editor for the past few years.

View all posts