Cyberattacks exploiting COVID-19

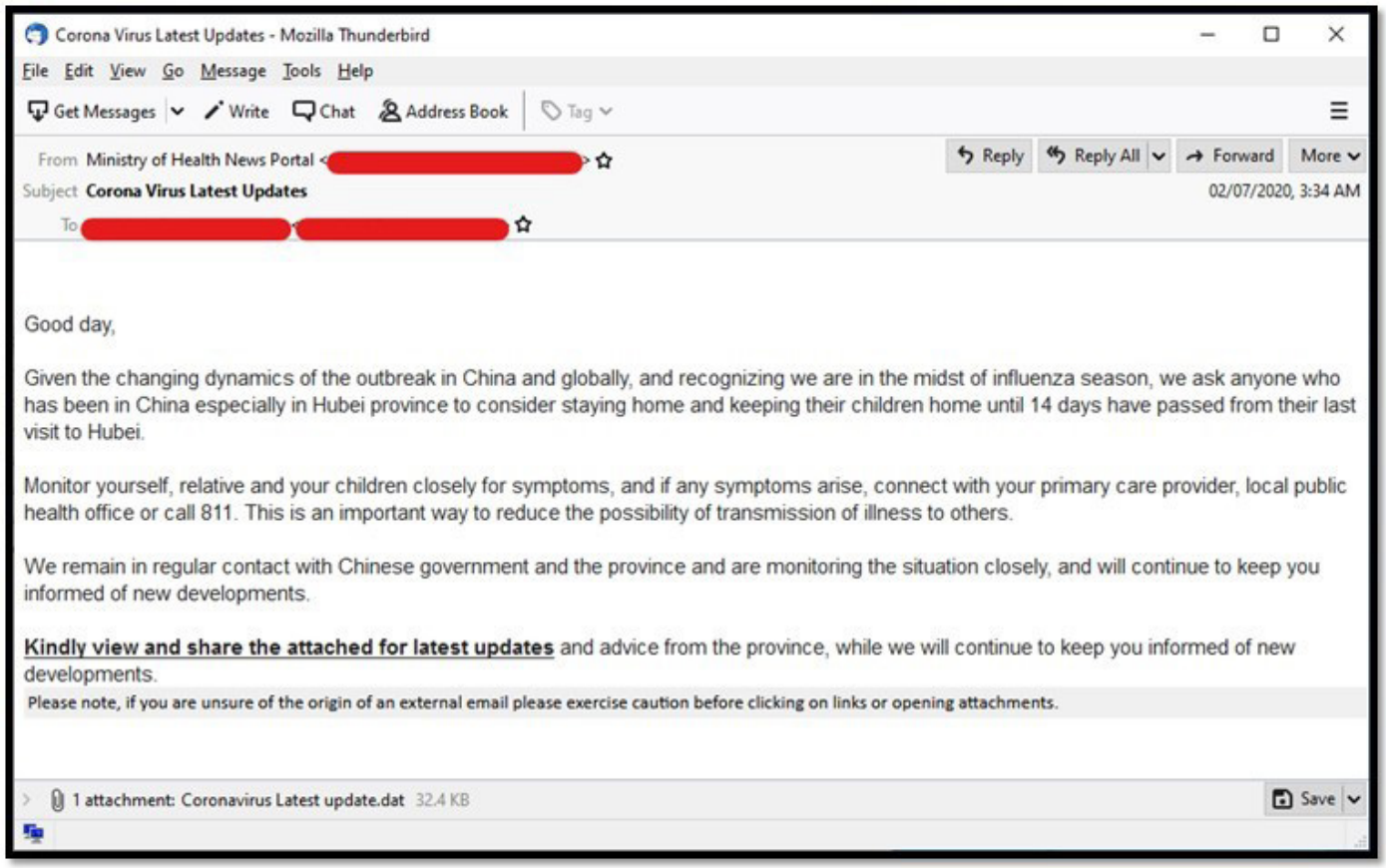
Cyberattack campaigns exploiting COVID-19 with global impact

The disease COVID-19 is being used as a hook for malicious social engineering campaigns, including spam, malware, ransomware and malicious domains. As the number of cases continues to grow by thousands, the campaigns that use the disease as a lure are also on the up. Panda researchers constantly search for samples in malicious coronavirus-related campaigns.

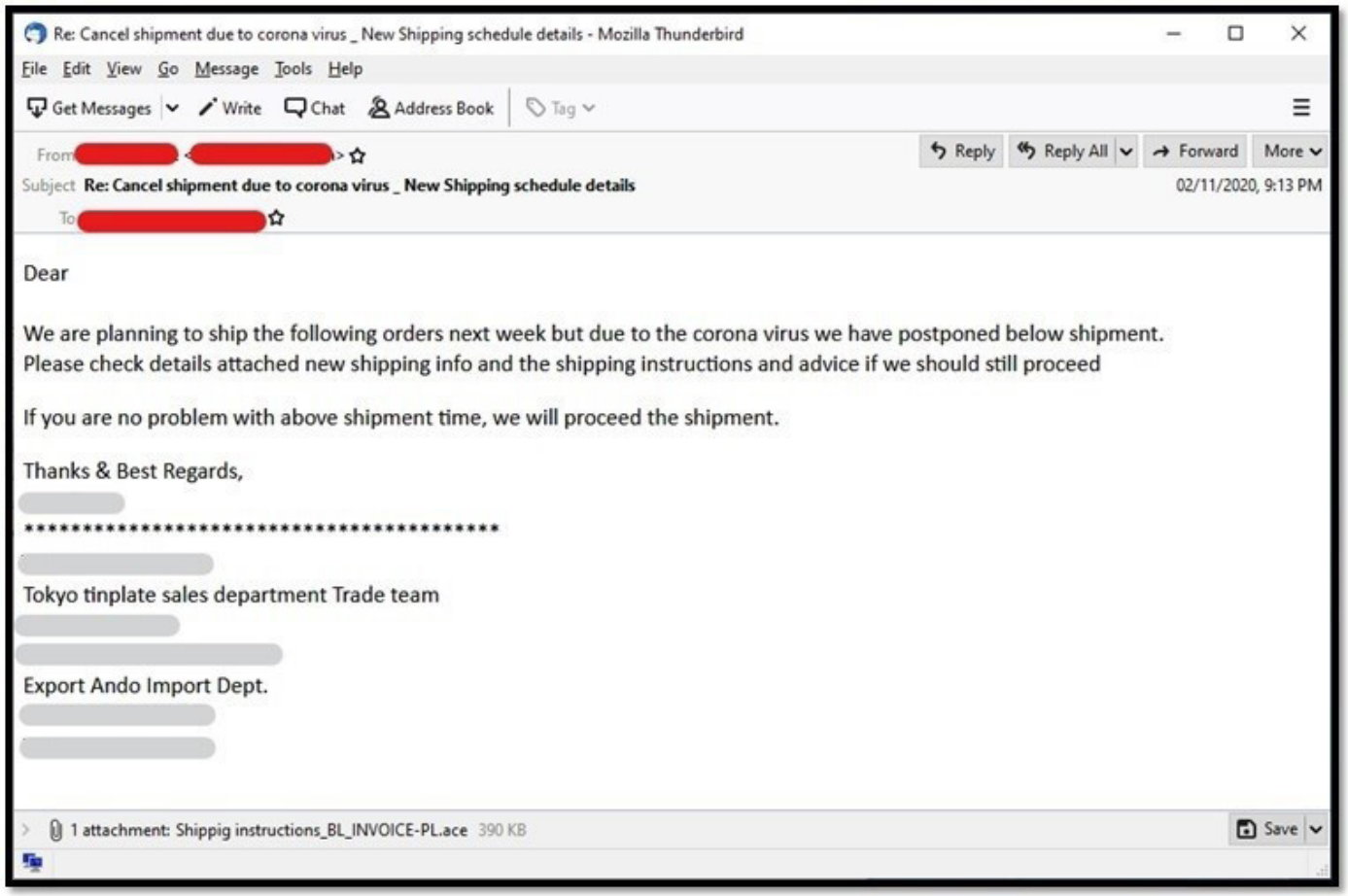
Coronavirus related spam

Panda researchers have detected emails sent and received all over the world, including countries such as the United States, Japan, Russia, and China. Many of these emails, supposedly from official organizations, claim to contain updates and recommendations related to the disease. Like most spam campaigns, they also include malicious attachments or website links.

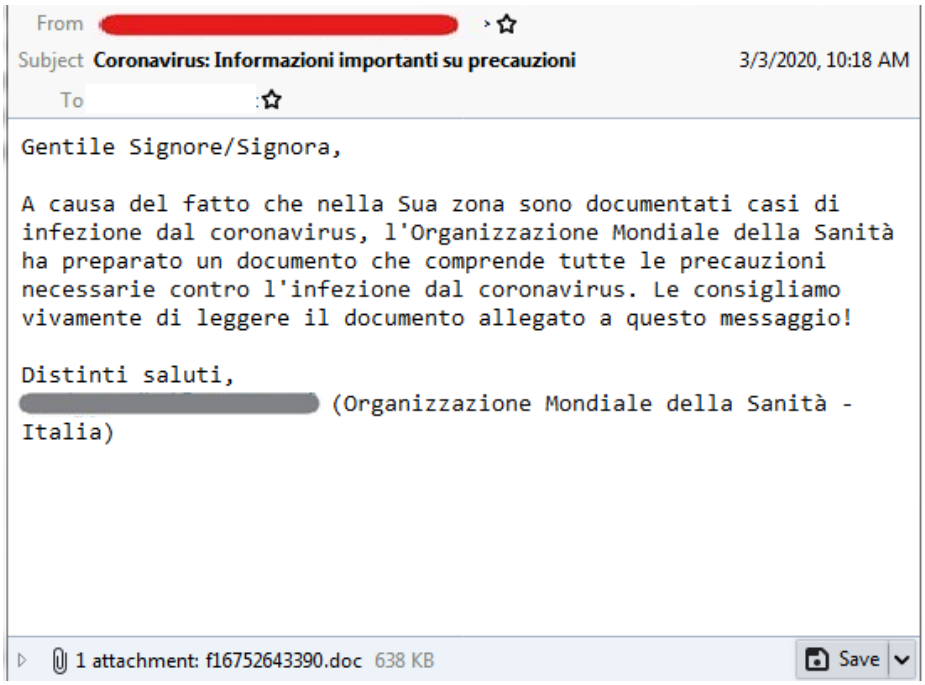
One example is a spam campaign with **"Corona Virus Latest Updates"** as the subject, purported to be sent from the Ministry of Health. It contains recommendations about how to prevent infection and comes with an attachment that supposedly contains the latest updates about COVID-19. However, it actually contains a piece of malware.



Other emails used in these campaigns, are related to product deliveries, which have supposedly been delayed or modified because of the spread of the disease.



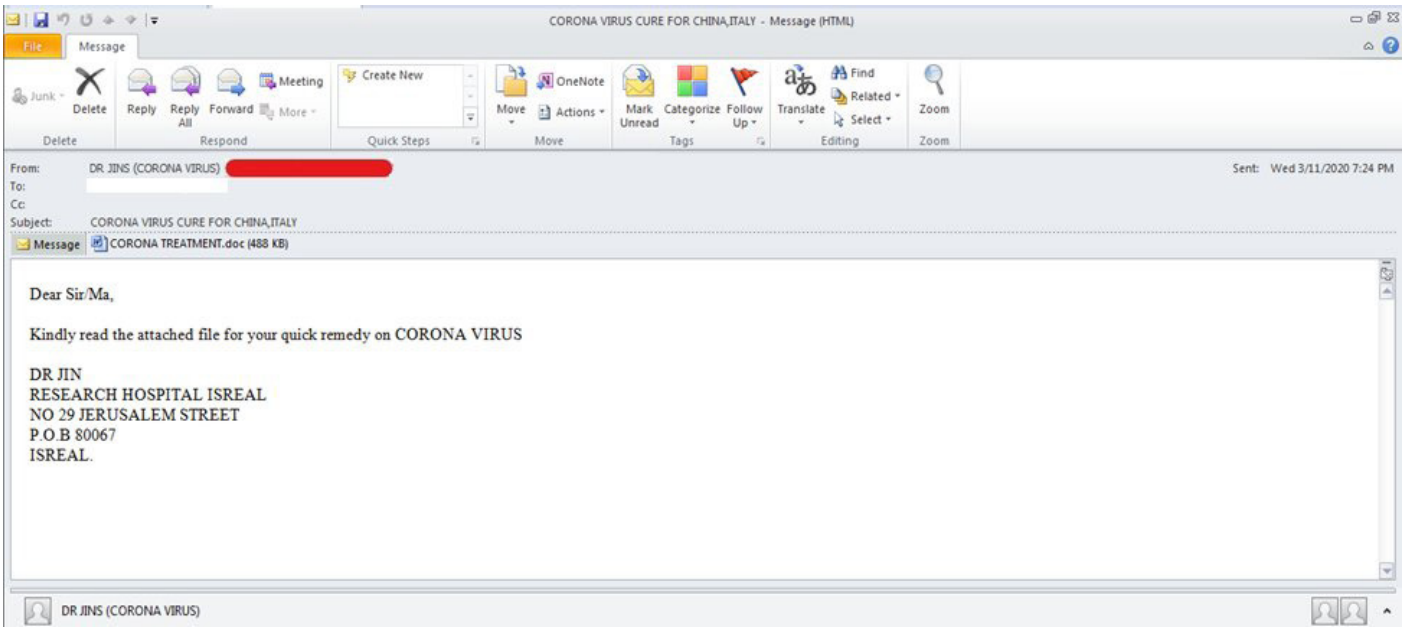
The following email in Italian refers to important information about the virus:



The following email in Portuguese promises news about a supposed vaccine for COVID-19.

Spam related to COVID-19 in Portuguese

There have been cases of Spam emails mentioning a cure for coronavirus in the subject, using this to try to get people to download the malicious attachment. This malicious attachment is sometimes **HawkEye Reborn**, a variant of the HawkEye Trojan, which steals information.



HawkEye Reborn spam

Indicators of compromise for the malicious attachment

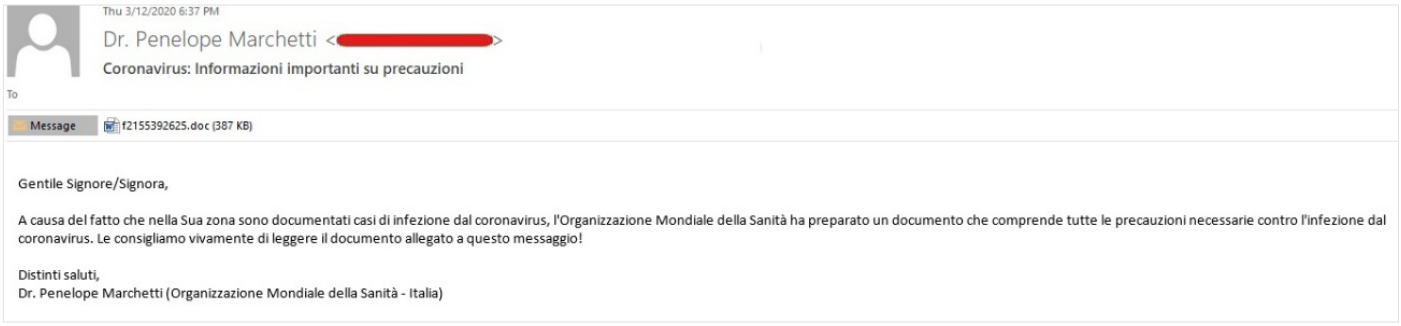
SHA-256
b9e5849d3ad904d0a8532a886bd3630c4eec3a6faf0cc68658f5ee4a5e803be

Italian spam with a COVID-19-related URL

The Indicators of compromise in this case are:

SHA-256
6cc5e1e72411c4f4b2033ddafe61fdb567cb0e17ba7a3247acd60cbd4bc57bfb
7c12951672fb903f520136d191f3537bc74f832c5fc573909df4c7fa85c15105

Another spam campaign has been seen targeting users in Italy, a country hit hard by the pandemic. This campaign includes “Coronavirus: important information on precautions” both in the subject and the body of the email. In the body of the email, the sender claims that the attachment is a document from the World Health Organization (WHO) and strongly recommends that readers download the compromised Microsoft Word attachment. The malicious file contains a Trojan.


Thu 3/12/2020 6:37 PM

Dr. Penelope Marchetti <[redacted]>

Coronavirus: Informazioni importanti su precauzioni

To

Message f2155392625.doc (387 KB)

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Sample of spam targeting Italian users.

When the document is opened, the following message is shown, prompting users to enable macros:

Attachment sample

Indicators of compromise (IOCs)

SHA-256
dd6cf8e8a31f67101f974151333be2f0d674e170edd624ef9b850e3ee8698fa2

Malware & CoronaVirus Ransomware

Thanks to our 100% attestation service, Panda laboratories has managed to identify and block the following malicious executables related to these campaigns:

File Name	SHA 256
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	ab533d6ca0c2be8860a0f7fbfc7820ffd 595edc63e540ff4c5991808da6a257d
	17161e0ab3907f637c2202a384de67fca 49171c79b1b24db7c78a4680637e3d5
	315e297ac510f3f2a60176f9c12fcf9 2681bbad758135767ba805cdea830b9ee
CoronaVirusSafetyMeasures_pdf.exe	c9c0180eba2a712f1aba1303b90cbf12c11 17451ce13b68715931abc437b10cd
	29367502e16bf1e2b788705014d0142 d8bcb7fcc6a47d56fb82d7e333454e923
LIST OF CORONA VIRUS VICTIM.exe	3f40d4a0d0fe1eea58fa1c71308431b5c2c e6e381cacc7291e501f4eed57bfd2
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	3e6166a6961bc7c23d316ea9bca87d82 87a4044865c3e73064054e805ef5ca1a
POEA Advisories re-2020 Novel Corona Virus.2.pdf.exe	b78a3d21325d3db7470fbf1a6d254e23d34 9531fca4d7f458b33ca93c91e61cd

Other researchers have seen cybercriminals taking advantage of online coronavirus monitoring maps, replacing them with fake websites that facilitate the download and installation of malware. Below are the hashes for these malicious applications:

SHA 256
2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d
13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e
fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8
126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040

A new variant of CoronaVirus ransomware was using a fake system optimization site to spread. Victims unknowingly download the **WSGSetup.exe** file from the fake site. This file acts as a downloader for two kinds of malware: The CoronaVirus ransomware and the password stealing **Trojan Kpot**.

This campaign is part of a recent trend seen in ransomware: it combines data encryption with information theft.

What' s more, another piece of ransomware, this time affecting mobile users, called **CovidLock** has also been spotted. This ransomware comes from a malicious Android app that supposedly helps track COVID-19 cases. The ransomware blocks its victims' cellphones, giving them 48 hours to pay **$100 in bitcoins** to regain access to their phones. Threats include deleting all the data on the phone and leaking details from their social media accounts.

Domains related to Coronavirus

There has also **been a notable increase** in the number of domain names using the word 'corona'. Below, we list some of the malicious domains:

- acccorona [.] com
- alphacoronavirusvaccine [.] com
- anticoronaproducts [.] com
- beatingcorona [.] com
- beatingcoronavirus [.] com
- bestcorona [.] com
- betacoronavirusvaccine [.] com
- buycoronavirusfacemasks [.] com
- byebyecoronavirus [.] com
- cdc-coronavirus [.] com
- combatcorona [.] com
- contra-coronavirus [.] com
- corona-blindado [.] com
- corona-crisis [.] com
- corona-emergencia [.] com
- corona explicada [.] com
- corona-iran [.] com
- corona-ratgeber [.] com
- coronadatabase [.] com
- coronadeathpool [.] com
- coronadetect [.] com
- coronadetection [.] com

How these attacks work

The fact is that all these attacks use entry vectors that could be considered "traditional". At Panda, we have these vectors more than covered with our Panda Endpoint Solutions. In these cases, the mechanisms used to detect and block the threats are the following:

- This service classifies every binary, only allowing it to execute if it is verified by our cloud-based artificial intelligence system, the managed **100% attestation service**
- Endpoint detection technologies, especially the detection of **Indicators of Attack (IoA) by behavior and context.**

From what we are seeing in our laboratories, the most common attack cycle is email/spam using social engineering technologies. These emails contain a dropper that downloads a binary here:

C:\Users\user\AppData\Local\Temp\qeSw.exe with the hash 258ED03A6E4D9012F8102C635A5E3DCD. In Panda's solutions, the detection for the dropper is a Trj/GdSda.A.

This binary encrypts the machine (process: vssadmin.exe) and deletes the shadow copies by invoking the process conhost.exe.

Official sources of IoCs

The Spanish National Cryptographic Center (https://www.ccn.cni.es/index.php/es/) has an exhaustive list of indicators of compromise (IoCs) at the level of hashes, IPs, and domains.

The information can be accessed here: https://loreto.ccn-cert.cni.es/index.php/s/oDcNr5Jqqpd5cjn

How to defend yourself against these and other cyberthreats

Thanks to the **100% attestation service,** which classifies all binaries before they can run, and blocks any malicious binaries, Panda' s advanced endpoint solutions are undoubtedly of great value in stopping these campaigns, as well as many others.

This service enables a highly efficient and unmanned mechanism for detecting and blocking malware and ransomware, even before it can run, regardless of whether they are new variants or new download domains, as is the case with the malware variants related to COVID-19.

Behavioral and contextual indicators of attack (IoAs) detect and block unusual behaviors on protected devices. These behaviors could include downloading an executable from a Word or accessing an unknown or malicious URL. Any attempt to compromise the device is immediately blocked, and the execution and connection of these malicious activities are stopped.


panda
30
year
anniversary