

Landscape Update: Coronavirus Cyber Threats

 proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update

March 18, 2020



Coronavirus Cyber Threat Landscape Update

Proofpoint researchers have tracked attackers leveraging the coronavirus pandemic since January 29. This blog serves as an update of the overall threat landscape and includes selected examples to highlight what we are seeing.

Currently, attackers are using coronavirus themes for nearly all types of attacks, including (but not limited to) [business email compromise](#) (BEC), credential phishing, malware, and spam email campaigns.

The targeting of these attacks has ranged from extremely broad to narrowly focused and campaign volumes have fluctuated between small and large. Attribution includes both well-known and unknown threat actors. Some of the well-known threat actors include TA505 and TA542.

We've observed attacks around the world, most notably in Italy, the Czech Republic, Japan, United States, Canada, Australia, and Turkey. In addition to English, attackers have used Italian, Czech, Japanese, Spanish, and French languages within their messages.

While all industries have been targeted, we've seen specific targeting of healthcare, education, manufacturing, media, advertising, and hospitality organizations in certain campaigns.

Attackers are actively abusing the names and logos of many companies and organizations within these campaigns in an attempt to manipulate recipients. Of particular note is the spoofing and brand abuse of national and international health organizations around the world, including the World Health Organization (WHO), the United States Centers for Disease Control (CDC), and Canadian and Australian national health organizations.

Threat actors have launched coronavirus campaigns to spread remote access Trojans (RATs), keyloggers, information stealers, and bankers. We are also seeing credential phishing campaigns with this theme. For example, we observed attempts to harvest credentials for Facebook, DocuSign, Microsoft Outlook Web Access (OWA), Microsoft OneDrive, and universities around the world.

We expect attackers will continue to leverage coronavirus themes in their attacks for some time to come. Proofpoint researchers will continue to track closely and provide updates on our blog and through our [Threat Insight Twitter handle](#).

Below are several notable examples of what we've seen.

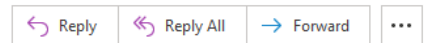
BEC Attempt: "People tested positive downtown so I can't go out right now"

Key Points: BEC attackers use the claim of positive coronavirus tests in their area to start email conversation.

Urgent Reply needed about corona virus



To Undisclosed recipients:



Mon 3/9/2020 12:19 PM

Hi

hope you are good today .

i will need you to do something for me urgently.

About 3 people has been tested positive of corona down town my area so i cant go out for now.

kindly reply back to me via email as my phone is faulty at the moment

Regards



BEC Attempt Summary:

This BEC email attempts to capitalize on current events and the global shift towards quarantine to prevent further spreading of coronavirus. BEC actors often try to convey a sense of urgency or immediate need. In this attack, the urgency is present in the subject line used here: "Urgent Reply needed about corona virus"[SIC].

BEC attacks are often delivered in stages. The first email sent is typically innocuous, meaning that they do not contain the attacker's end goal. The attackers craft plausible scenarios in hopes the recipient will reply. Once they're on the hook, the attacker will send their true ask. (I need you to buy gift cards, wire transfer funds, etc.)

These coronavirus-themed BEC attacks often come with spoofed display names, which are likely real people known to the recipient. In the body of this message, the actor attempts to eliminate the possibility of voice-verification, in hopes of ensuring a higher success rate, by saying their phone is "faulty at the moment."

Credential Phish: Microsoft Office

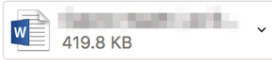
Key Points: Attackers use credible, customized, fake internal emails for credential phishing attacks targeting the healthcare industry.

Update On Novel Coronavirus(2019-nCoV)



Monday, February 10, 2020 at 8:35 PM

[Show Details](#)



[Download All](#) [Preview All](#)

LETTER FROM THE PRESIDENT

Dear colleagues,

I'm writing about the outbreak from CORONAVIRUS 2019-nCoV. Like other [redacted], on 28 January 2020, [redacted] called for the temporary suspension of all planned travel to China for study, research or conferences until further notice.

On December 31, 2019, the World Health Organization was informed of a cluster of cases of pneumonia of unknown cause detected in Wuhan, Hubei Province of China. Chinese health authorities identified a novel Coronavirus (referred to as 2019-nCoV) as being responsible for the respiratory outbreak.

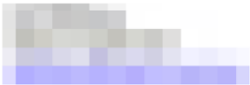
The main reason for this decision is not only the risk of infection by 2019-nCoV, but also the unpredictable nature of the outbreak, the associated risk of social unrest in the affected areas or quarantine restrictions, which could make it impossible to return home.

The steps you can take to protect yourself from getting infected with 2019-nCoV are attached in this email and all employees including full-time or part-time employment are required to go through the attachment.

We hope that the situation will improve as soon as possible,

Best Regards

Sincerely,
President



Microsoft Office Credential Phish Summary:

These specific Coronavirus cyber attacks targeted companies in the healthcare industry. Our researchers found that the emails were highly customized to each target to increase their credibility. They claimed to be from the targeted company's actual president and used the targeted company name and president's name multiple times in the email.

The messages conveyed information about halting all travel to China and contained an attached Word document with a link inside of it. If a user clicked the link, they would be brought to a spoofed Microsoft Office branded credential phishing site that asks for email login and password.

Credential Phish: Outlook Web Access (OWA)

Key Points: Attackers use an employee survey about coronavirus to target Outlook Web Access credentials.

RE: IT-Service desk: Coronavirus notice for all employee

**Weerheim - Dooge, Joke** <J.Weerheim_1@careyn.nl>

Tuesday, March 3, 2020 at 8:44 AM

[Show Details](#)

Van: Weerheim - Dooge, Joke
Verzonden: dinsdag 3 maart 2020 14:22
Aan: Weerheim - Dooge, Joke
Onderwerp: IT-Service desk: Coronavirus notice for all employee

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link [SURVEY/SEMINAR](#) to participate in the survey and register for the seminar.

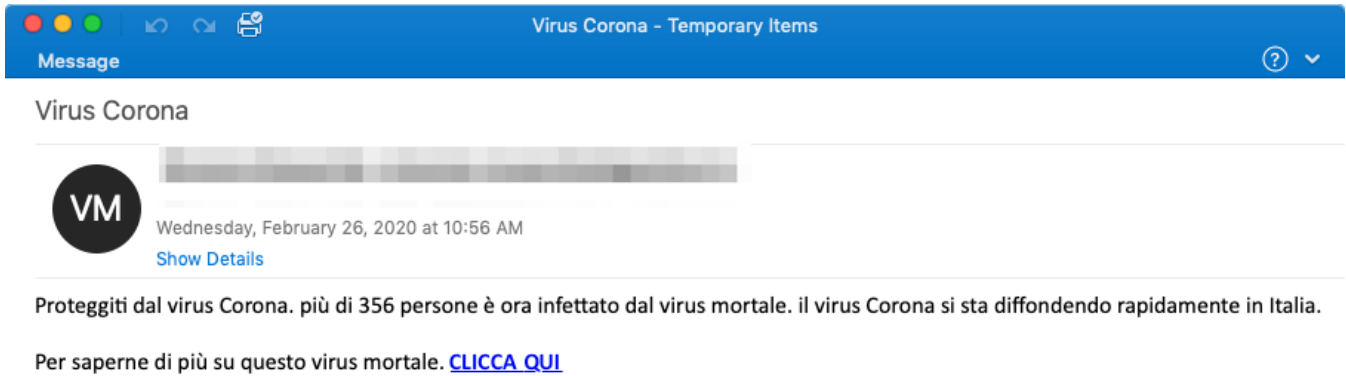
Best Regards
IT-Service desk

Outlook Web Access Credential Phish Summary:

These Coronavirus cyber threats claim to be from an organization's IT department and poses as an awareness and education email for employees around coronavirus. The email asks the recipient to click on the link to take a survey and register for a health safety awareness seminar. If a recipient clicks the link, they're taken to a credential phishing page that asks for their Outlook Web Access (OWA) credentials.

Credential Phish: Italian Email Credential Phish

Key Points: Attackers use an Italian language lure around the spread of coronavirus to capture email credentials.



Italian Email Credential Phish Summary:

On February 26, 2020, Proofpoint researchers observed an email credential phishing campaign targeting Italy. It was written in Italian language and urged recipients to protect themselves as the virus was spreading and many were infected. If they clicked on the URL in the email, they were presented with an email credential phishing page. The credential phishing landing page also used custom coronavirus-themed graphics.

Malware: Ostap / The Trick Banker

Key Points: Campaigns targeting Italy and Czech Republic with WHO lures.

Coronavirus: Informazioni importanti su precauzioni



Dr. Penelope Marchetti

Thursday, March 12, 2020 at 7:10 AM

[Show Details](#)



[Download All](#)

[Preview All](#)

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)

Ostap / The Trick Banker Malware Summary:

In March 2020, we've seen multiple instances of attackers attempting to deliver malicious Word macro documents in Italy and Czech Republic. These emails claim to come from local medical professionals, for example, "Dr. Penelope Marchetti (World Health Organization - Italy)" with an attachment that contains an update on infection cases in their area.

If the recipient enables macros from the attachment, the documents would drop and run Ostap JavaScript downloader, which in these instances downloaded The Trick "red5" banker.

To note, Italy is currently one of the most targeted regions we've observed within this attack theme, with multiple malware and phishing threat actors attempting to deliver malicious emails using Coronavirus lures.

Malware: Get2 Downloader

Key Points: Threat actor TA505 targets pharmaceutical and manufacturing industries in the United States.

COVID-19 Everything you need to know



John DeFranco

Tuesday, March 10, 2020 at 7:28 AM

[Show Details](#)

! This message is high priority.

How to Protect your friends from nCov 2019 FAQ

There are more than 75,000 infected COVID-19 cases all around the world!

[COVID-19-FAQ](#) - uploaded with iCloud Drive.

Regards,
John DeFranco

Get2 Downloader Malware Summary:

On March 10, 2020, Proofpoint researchers observed thousands of emails primarily targeting pharmaceutical and manufacturing companies in United States. The emails claimed to contain information about how to “protect your friends” from coronavirus and urged the recipient to click on a link.

If the recipient clicked on the link, they would be taken to a web page where they had to click on another link, which would then download a malicious Excel document. After downloading the malicious Excel document, if the recipient also enabled macros, the macros executed an embedded Get2 loader. Get2 typically downloads SDBbot RAT.

While the email lure is simple and not particularly compelling compared to others we observed, this campaign was distributed by [TA505](#), a threat actor [tracked](#) by Proofpoint. The group is known for their large campaigns, experimentation with a variety of delivery mechanisms, and distribution of ransomware, bankers, and RATs.

Malware: Urnsif Banker

Key Points: Threat actor TA564, who regularly targets Canada, launches email campaign targeting “parents and guardians” and spoofs Public Health Agency of Canada.

Update: Coronavirus (COVID-19) # 55711



Public Health Agency of Canada <pablichealth@██████████>

Tuesday, March 10, 2020 at 2:15 PM
[Show Details](#)

March 10, 2020

Dear Parents and Guardians,

We are writing to provide you with another update from Public Health Agency of Canada with regards to the novel coronavirus (COVID-19). Below, you will find an updated letter from Medical Officer of Health with the latest information:

Letter from Medical Officer of Health:



Thank you.

Urnsif Banker Malware Summary:

Proofpoint researchers observed on March 10, 2020 an email campaign targeting Canadian users claiming to be from the Public Health Agency of Canada. It addressed "parents and guardians" with an update from the spoofed health agency. This clearly sought to leverage parents' emotions about their children's wellbeing and increase the attack's success rate.

The email contained a URL, linking to a compressed Microsoft Word document (named Coronavirus_disease_COVID-19__461657952561561.doc) with macros. If the recipient enabled the macros, they would download and install Urnsif banker.

We attribute this activity to threat actor TA564. This threat actor typically targets Canada with false shipping lures, such as CanadaPost and DHL, and have attempted to deliver Ursnif, DanaBot, and Nymaim in the past.

Malware: GuLoader and Agent Tesla

Key Points: Campaign exploits Equation Editor vulnerabilities to load GuLoader and Agent Tesla.

coronavirus finally struck america And European Continent



Thursday, March 5, 2020 at 9:28 AM
[Show Details](#)



[Download All](#) [Preview All](#)

Coronavirus Finally Hit us Be warned !!!

FYI; kindly see attached for the affected States in America and other Countries; areas; Shops and infected persons newly affected by the new Coronavirus in our Country. Kindly spread the information to family and friends for their safety.

Regards;
Nico
Risk Manager

GuLoader and Agent Tesla Malware Summary:

Proofpoint researchers found this email, dated March 5, 2020, that seeks to capitalize on fears around the spread of coronavirus in the United States. It contained a message about affected areas in America (and the European continent), including shops. The malicious attachment titled "COVID 19_List_cities_names.xlam" supposedly contained a list of impacted city names.

When the recipient opened the malicious attachment, it attempted to exploit Equation Editor vulnerabilities to download GuLoader, which in turn would download Agent Tesla.

Malware: Remcos

Key Points: Campaign impersonating Philippines Customs to deliver Remcos.

E-Mail Alert for COVID-19 Importation Regulation



cprs@customs.gov.ph

Sunday, March 15, 2020 at 9:52 PM

Show Details

Date: Mon Mar 16 08:02:23 PHT 2020
Subject: Importation Regulation For COVID-19

Sir/Madam,

This is to inform you that Bureau of Customs due to COVID-19 there will be New Implement on Importation Regulation of goods into Philippines.

Please find attachment is the guide lists of Goods Suspended and New Importation Regulation.

Please be guided accordingly.

Thank you!
BUREAU OF CUSTOMS



Remos Malware Summary:

On March 16, 2020 Proofpoint researchers observed an email campaign targeting various international companies. The emails impersonated the Philippines customs agency and claimed to contain information about new regulation of imports as well as suspended goods. This was an interesting lure since trade suspensions and regulations have potentially greater impact compared to even travel restrictions.

These emails contained Microsoft OneDrive URLs leading to a compressed Remcos RAT executable.

Spam: Pandemic Survival Course

Key Points: Spam campaign promoting a survival course containing everything you supposedly need to know about the coronavirus pandemic for \$37.

Corona worse than Ebola?



Pandemic Survival <PandemicSurvival@pandemics.bid>

Thursday, March 12, 2020 at 9:13 AM

[Show Details](#)

To protect your privacy, some pictures in this message were not downloaded.

[Download pictures](#)

If you're counting on your government to shield you from the deadly coronavirus, I have a message for you...

Don't be silly.

[They wouldn't know how even if they tried.](#)

Leaked private meetings between U.S. health officials tell us.... they are in a panic.

Not only do they not know what to do...

They're not really sure how many people are infected.

Reports from the United States range from 35 to 105.

They are at a loss.

[Corona worse than Ebola?](#)

But you don't have to be.

There is 1 thing you can do...right now...to save yourself.

[You have to see this](#)

1 thing to protect yourself from the deadly coronavirus. And I don't mean masks (they can't protect you if a droplet gets in your eyes).

Smallpox killed 300 million people and had a LOWER mortality rate than coronavirus.

That's the entire population of the United States and the coronavirus is playing out a very similar pattern.

Do you realize that once one of your family members gets it you won't be able to take care of them or even see them.

Because they could spread it to you.

Imagine not being able to hold or even touch your sick child. [Don't let it happen to you](#)

Wilson

P.S. That video is making WAVES on the internet. No offense, but you're probably the last person to see it.

BREAKING:
Military Source Exposes Shocking TRUTH About Coronavirus And The "1 Thing" You Must Do Before It's TOO LATE

CORONAVIRUS SPECIAL REPORT

CLICK TO PLAY

Watch This Important Health Bulletin Before It's TOO LATE

buygoods Customer Support

Secure Order Form

PAYMENT DETAILS

United States | Please select

Your billing address

Your billing city

Zip/Postal code here

Email

Name as it appears on your card

Phone

Shipping same as billing

ORDER DETAILS

DIGITAL DOWNLOAD | Pandemic Guide

USD - US Dollar

Your Price:	\$37.00
Taxes:	\$0.00
Shipping:	\$0.00
Total:	\$37.00

100% MONEY BACK GUARANTEE 60 DAYS

We put our hearts and souls into building **BuyGoods** as the most safe, friendly and reliable online shopping destination. You are protected by our **60 days** no questions asked **money back guarantee**.

SECURITY SCANNED TRUST GUARDED 03-08-20

BUSINESS VERIFIED TRUST GUARDED 03-08-20

Pandemic Survival Course Spam Summary:

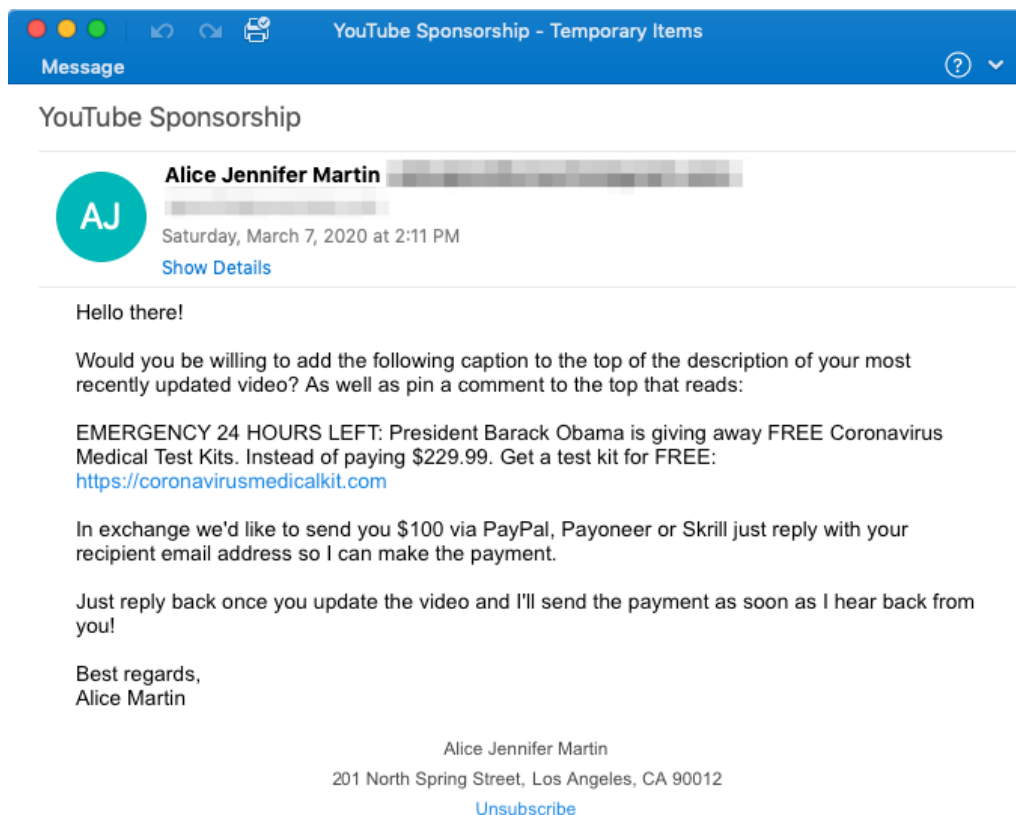
In March 2020, Proofpoint researchers observed multiple spam campaigns peddling an informational course for US\$37. The recipient must first watch a 30+ minute long video before getting the link to purchase the course.

The email and the video try to seed fear, uncertainty, and doubt into the recipient about the government's ability to respond to the situation. They describe a coming pandemic and other events (millions of people dead, forced quarantine by the military, drug companies experimenting on humans with vaccines and so on).

The course supposedly offers information around dozens of topics such as: How to make a hazmat suit; should you own a gun; how to keep the army out of your home; what to do if urban warfare breaks out; what to do if an infected neighbor knocks on your door. We did not verify what happens after the payment, but we recommend to everyone to keep their money and not take the bait.

Spam: Coronavirus Testing Kit


Key Points: Spam campaign asking media and advertising companies to promote a malicious website that supposedly sells testing kits in exchange for US\$100.



YouTube Sponsorship - Temporary Items

Message

YouTube Sponsorship

 **Alice Jennifer Martin**

Saturday, March 7, 2020 at 2:11 PM

[Show Details](#)

Hello there!

Would you be willing to add the following caption to the top of the description of your most recently updated video? As well as pin a comment to the top that reads:

EMERGENCY 24 HOURS LEFT: President Barack Obama is giving away FREE Coronavirus Medical Test Kits. Instead of paying \$229.99. Get a test kit for FREE:
<https://coronavirusmedicalkit.com>

In exchange we'd like to send you \$100 via PayPal, Payoneer or Skrill just reply with your recipient email address so I can make the payment.

Just reply back once you update the video and I'll send the payment as soon as I hear back from you!

Best regards,
Alice Martin

Alice Jennifer Martin
201 North Spring Street, Los Angeles, CA 90012
[Unsubscribe](#)

Coronavirus Testing Kit Spam Summary:

In early March, Proofpoint researchers observed a small spam campaign targeting media and advertising companies in the United States. The email did not try to get the recipient to open the malicious URL, but instead asked the recipients to spread a website URL to their audience. Specifically, it asked them to place the URL and a short message on top of their most recent YouTube video description. The sender offered a payment of \$100 in exchange for this.

The website, coronavirusmedicalkit[.]com, offered to sell free COVID-19 testing kits. However, at the end of the ordering process a \$10 fee was added (likely for shipping). As Better Business Bureau [put it](#), a lot of times "these phony sellers take victims' money and never deliver anything at all... These sites use tricks like limited time deals to entice you into ordering more." This campaign is interesting because we do not often see direct outreach like this via email.

Spam: Masks

Key Points: One of the most common spam types with Coronavirus as a lure are offers for masks.

Message Get your Corona-virus Mask while supplies last! - Temporary Items


Get your Corona-virus Mask while supplies last!

Corona-virus Mask <verification@groundsnack.icu>
Wednesday, March 11, 2020 at 5:22 AM
[Show Details](#)

Get your Corona-virus Mask while supplies last!


[Check it Out Here](#)

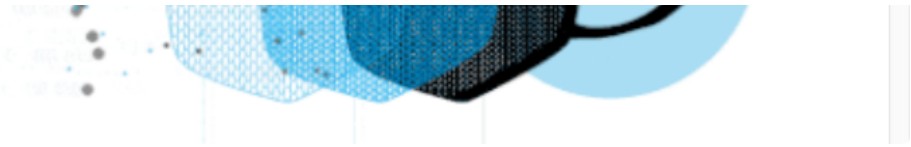
[Protect Yourself and Your Family From Deadly Airborne Viruses](#)



Are you afraid of air spreading diseases and viruses?

Most of us are. The deadly coronavirus has infected more than 17000 and killed at least 1200 since its discovery in the Chinese city of Wuhan in late December. Infection is spreading at an alarming fast rate.





Masks Spam Summary:

The sale of masks is one of the most popular types of spam campaigns capitalizing on the coronavirus situation by volume. In this example, the email urged recipients to act urgently while supplies last. It offers to sell mask for \$49 each. Once again, as the BBB article puts it, recipients are likely to never receive anything if they pay.

Conclusion

This sampling shows just how broad and diverse the Coronavirus cyber threat landscape has become. Attackers of all kinds across the globe are now using coronavirus for nearly every type of attack possible.

These examples are just a fraction of what our researchers have seen. We are continuing to monitor closely and will continue to update with notable changes in attacks, attacker tactics, or trends in the threat landscape.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
4616c3a50e0393ababc925b496f04f3687664e9d1c4b7966485a7a9124047214	SHA256	Word document delivered in the Italian Ostap campaign in 2020-03-12
hxxp[:]//www[.]agt[.]net/~mnpicker/2jgmu9r/h9a6kn.html	URL	Example URL leading to Get2 on 2020-03-10
hxxp[:]//adsign[.]ik/wp-admin/tkennedy.php?t=[Redacted Base64]	URL	Example URL leading to Tordal on 2020-03-11
hxxp[:]//davidrothphotography[.]com/zHzrr	URL	Example URL leading to Ursnif on 2020-03-10
hxxps[:]//bitbucket[.]org/example123321/download/downloads/foldingathomeapp.exe	URL	URL hosting RedLine on 2020-03-07
4f630d3622d1e17c75aac44090b3b5bd47d5b2ae113434cde5708bbb7cffef49	SHA256	COVID 19_List_cities_names.xlam attachment leading to GuLoader & AgentTesla on 2020-03-05
c9a8dd42a46e2c6849564576f96db6741ad0036726f98d7b43641907f953d3f3	SHA256	"Rapport sur les coronavirus.doc" attachment leading to Ave Maria of 2020-03-06
hxxps[:]//toyswithpizzazz[.]com[.]au/service/coronavirus	URL	OWA phish on 2020-03-03
Www[.]pandemicsurvival[.]bid	Hostname	"Pandemic Survival" Course Spam on 2020-03-07

coronavirusmedialkit[.]com	Domain	“Coronavirus Testing Kit “ Spam on 2020-03-04
groundsnack[.]icu	Domain	Mask Spam on 2020-03-11
