Navigating Cybersecurity During a Pandemic: Latest Malware and Threat Actors

umbrella.cisco.com/blog/navigating-cybersecurity-during-a-pandemic-latest-malware-and-threat-actors

April 1, 2020

The coronavirus (COVID-19) outbreak tops all the news, google searches, and social media alerts for good reason. Globally, we need to stay informed of the latest news with this health crisis. However, it's also in the news due to malicious threat actors using COVID-19 as a lure to trick people into giving up account credentials, or to download malware.

In this blog post, we're going to discuss the latest ways that we've seen threat actors using the current health crisis in malicious campaigns, and the increase in Internet requests related to COVID-19 material.

Mass Information

Threat actors often use the latest world events, popular news headlines, holidays etc. as themes for malware content in order to stay relevant and entice victims to visit malicious websites or open malicious attachments in email. Given the global reach and urgency of the current health crisis, it's not surprising that COVID-19 has become a means for threat actors to deliver their latest malicious content.

Earlier this month, Brian Krebs reported on the use of fake coronavirus live update style maps to spread the AzorUlt information stealing trojan. The public is very interested in staying up to date on where the latest COVID-19 cases are happening around the world. If

we use Cisco Umbrella Investigate to look at the amount of query traffic seen on our resolvers going to one of these domains hosting a malicious live update map, you can see a spike in requests to this domain starting on March 11th, and continuing to gain more queries and maintain a steady flow of requests.

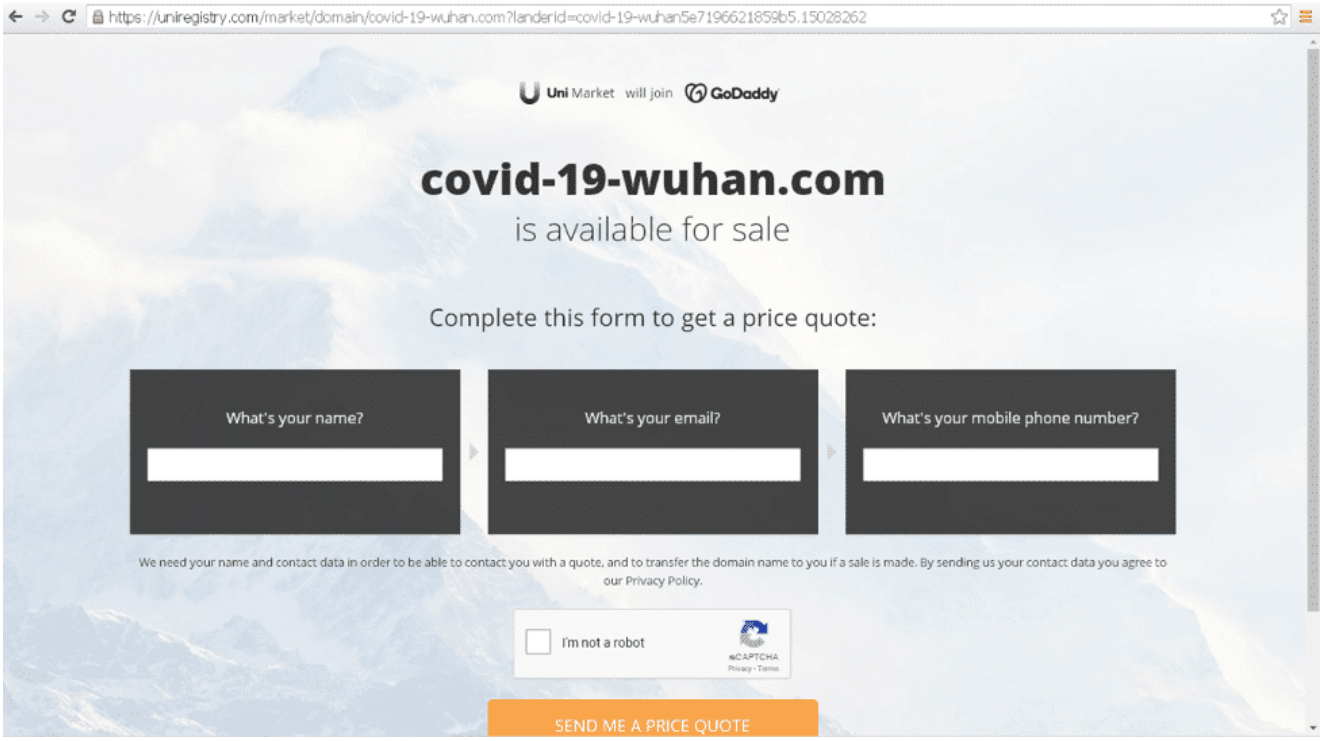
Investigate shows query traffic to a domain hosting a malicious COVID-19 map

A Surge in New Domains

We have certainly seen a surge in Internet requests to domains that include the word ‘covid’ or ‘corona’ over the past two months. On February 19, our enterprise customers made 562,144 queries to 8,080 unique domains containing these keywords. We saw an increase of 1,907% in requests being made by March 19th, from 11,287,190 requests, across 47,059 domains containing these keywords. 4% of these 47k domains were blocked as malicious sites.

Below is a list of popular keywords we’ve seen used together with corona, virus, and covid for new domain registrations:

- wuhan
- clinics
- lab
- tests
- selftestkit
- purchase kits
- helpline



A domain for sale using the keywords covid-19-wuhan

Malspam Attacks

Threat actors continue to use email as an infection method, with malicious documents or embedded malicious links. One approach is disguising the email as coming from the World Health Organization.

The emails state that the attachment contains important safety measures as directed from the WHO. These attachments have been seen to be an archive file, pdf, or doc.

Some of the malware threats that we're tracking associated with COVID-19 scams are highlighted below.

Kpot

Description: Kpot is an information stealer that steals user data and account credentials. It is very easily available in various underground forums for a price of around $100 USD.

Nanocore

Description: NanoCore RAT is a Remote Access Trojan which was first spotted in 2013. Since then, it has been available on the Dark Web. This trojan can be modified by its users as per their needs. The malware is capable of registry editing, process control, upgrade, file transfer, keylogging, and password stealing.

Guloader

Description: GuLoader is a downloader, written partly in VB6, which typically stores its encrypted payloads on Google Drive or Microsoft OneDrive. It is usually distributed as a portable executable (PE) file that is often observed embedded in a container file such as an .iso or .rar file. It is used predominantly to download Remote Access Trojans (RATs) and information stealers such as Agent Tesla, FormBook, NanoCore RAT, Netwire RAT, Remcos RAT, Ave Maria/Warzone RAT and Parallax RAT.

Trickbot

Description: TrickBot was first seen in 2016 and is a banking trojan with advanced browser manipulation techniques, server-side injections and redirection techniques. It has most famously been associated with malspam spread through the Emotet botnet and Trickbot's Command and Control servers have been seen as IOCs during investigations of Ryuk ransomware infections. Trickbot has the ability to steal email credentials and address book information that is used to send malspam from the affected accounts. In 2020, Trickbot began to target Active Directory DCs and bypass Windows UAC elevated privlege alerts. Trickbot can spread laterally through an internal network.

Formbook

Description: Formbook is a trojan information stealer spread through malspam with malicious document or archive attachments. It was first observed in 2017. It operates with the Malware-as-a-service (MaaS) model making it easy for cyber criminals to operate.

Netwire

Description: NetWire is a remote access trojan (RAT) which is widely used by cybercriminals since 2012. NetWire has a built-in keylogger that can capture inputs from peripheral devices such as USB card readers. Other targets include credentials for online accounts and applications such as email, property management systems (PMS), and internet browsers. Other sensitive information typed by the user, including Social Security numbers, phone numbers, addresses, and birthdates can also be compromised. It was used in attacks against banks and healthcare companies and scammers to remotely control infected systems.

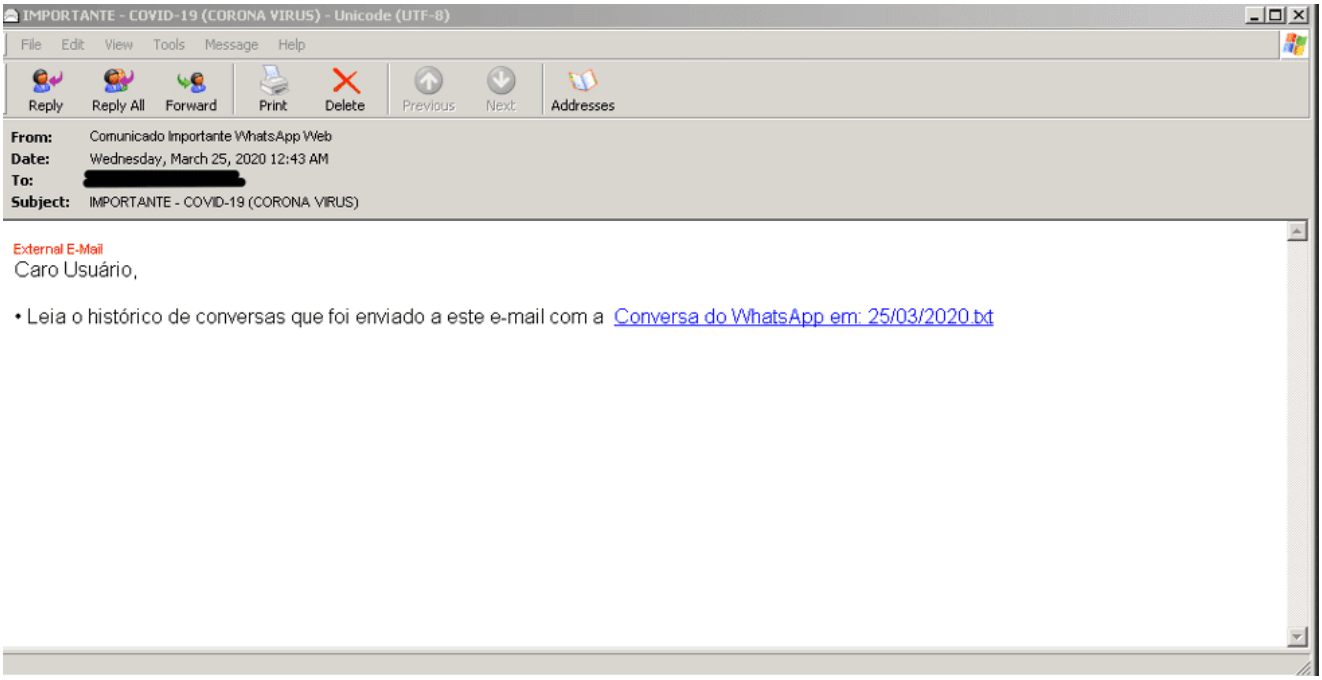
MetaMorfo

Description: Metamorfo is a banking trojan first seen in April 2018. Metamorfo's primary target location at the onset was Brazil. Today, it's targets have spread to USA, Chile, Spain, Mexico and others. The trojan gathers financial information, credit card numbers, and personal data.

MetaMorfo: 'Important Information'

We're going to look into a malspam campaign that dropped the MetaMorfo payload.

The targets of this malspam campaign were primarily Brazilian citizens. The emails contained a malicious attachment when opened that would lead to the download of a zip archive. This file starts the malicious process to drop MetaMorfo onto the victim's system.

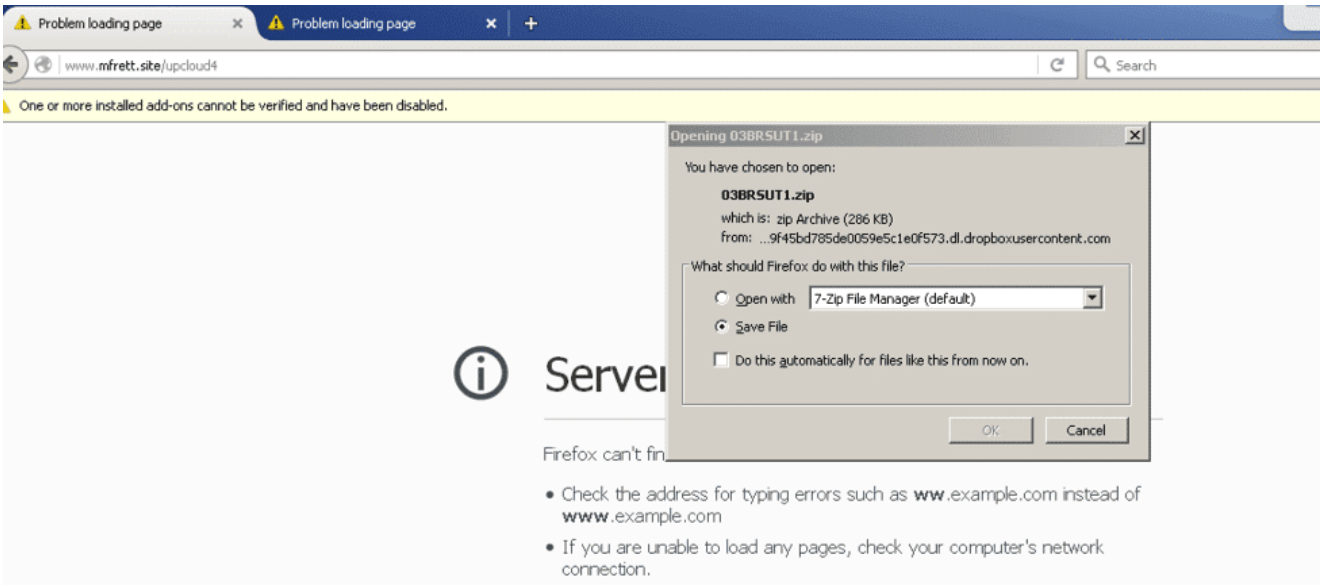


English Translation:

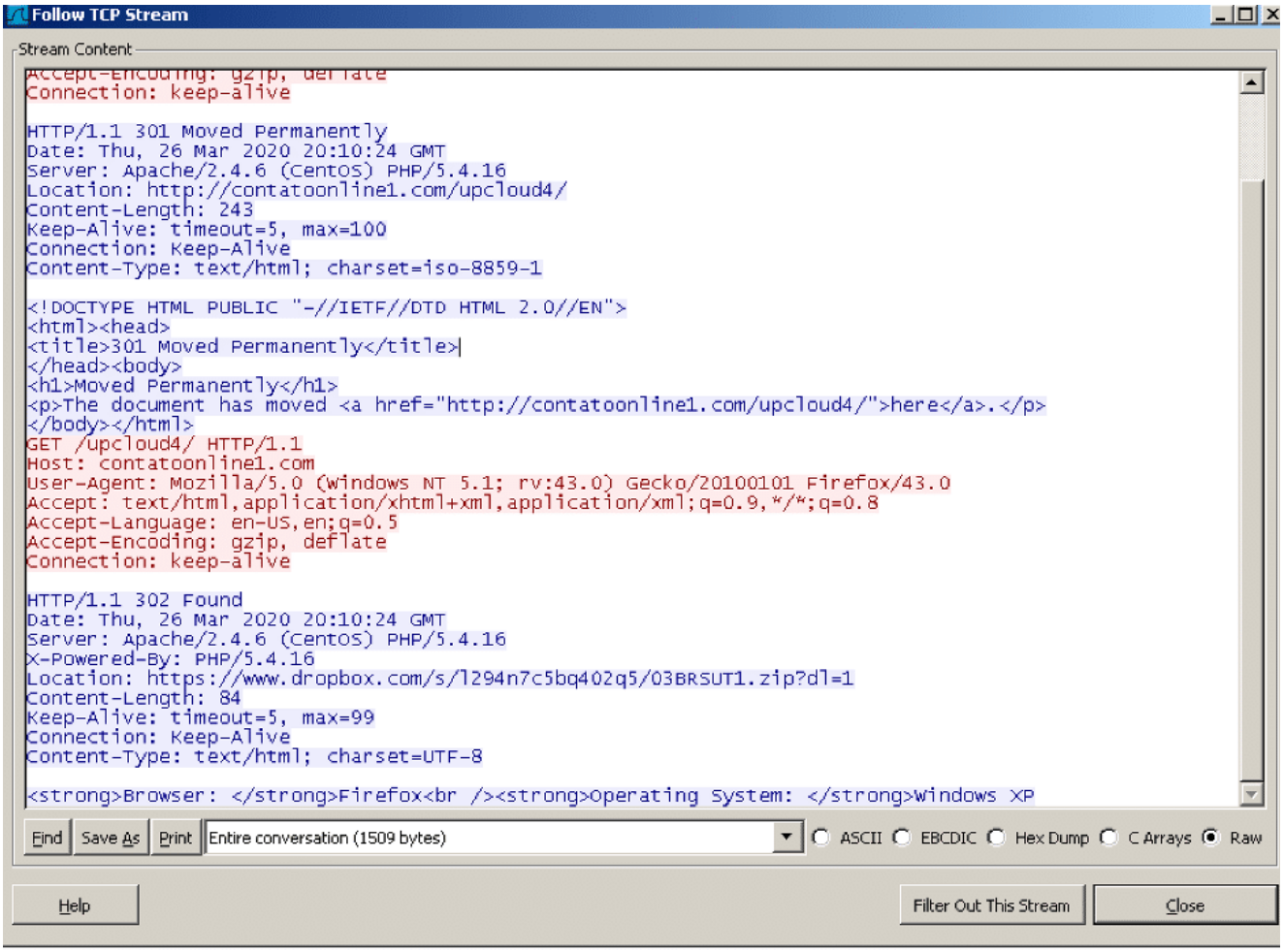
Dear User,

• Read the conversation history that was sent to this email with WhatsApp Conversation at: 03/25/2020.txt

The hyperlink leads to:
hxxp://www.servicosfcporto[.]com/upcloud7?WhatsApp_Historico_de_Conversas?whatsapphistorico/index.html?visualizar=c06e8cf10aeaf00c33360d2b2bfb6792

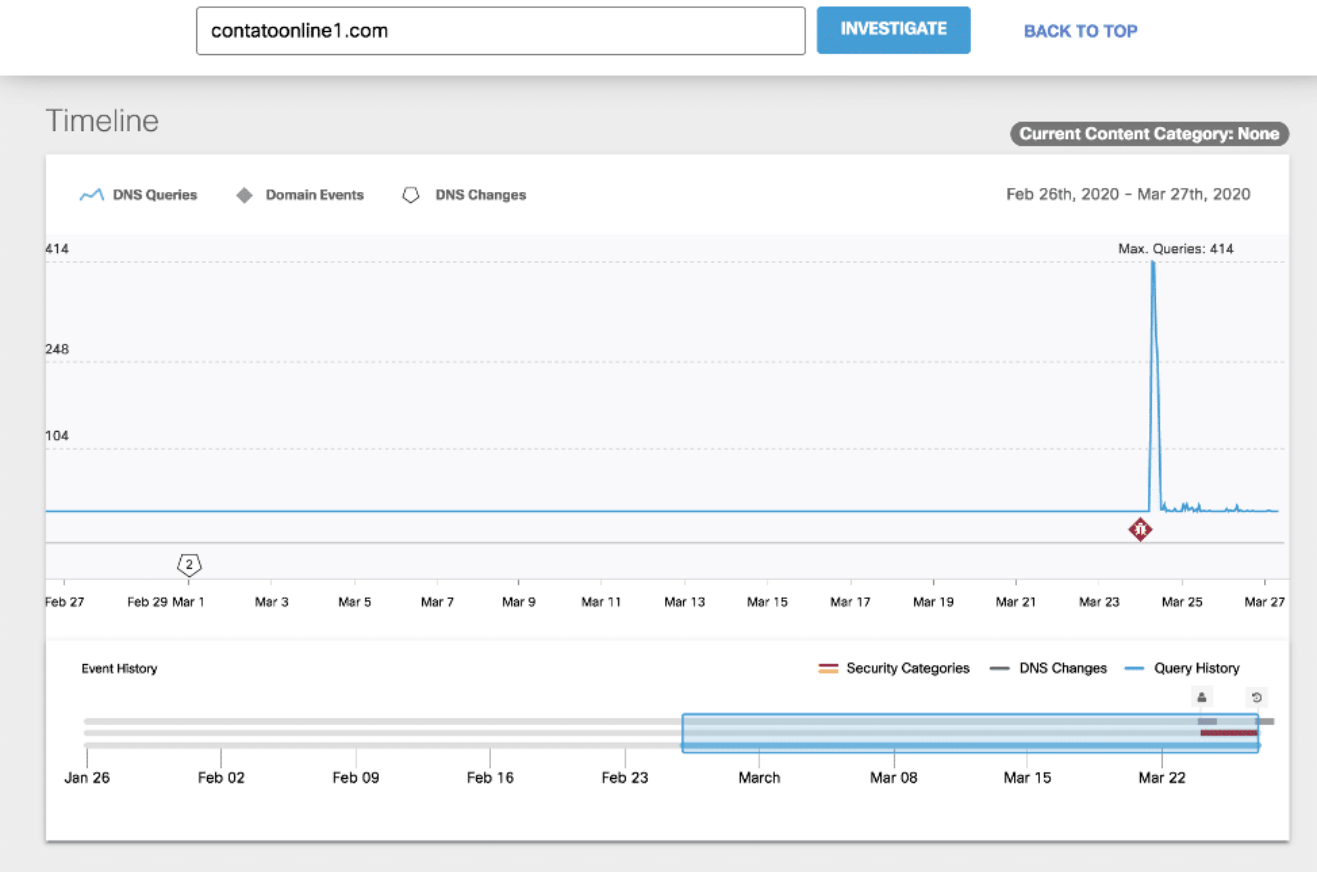


One of the dropper/redirect domains redirecting to download malicious content from Dropbox

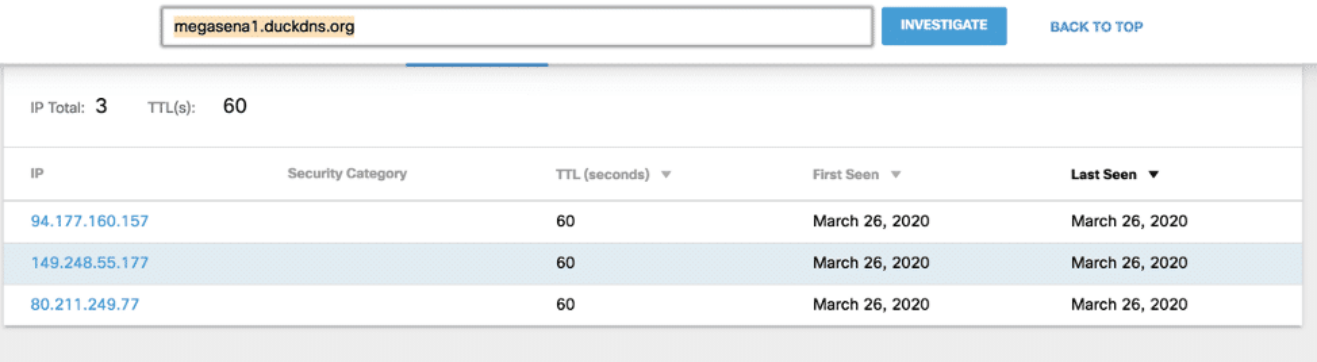


A 301 call redirect from one of the observed domains to download content from Dropbox

Cisco Umbrella was able to detect the redirect/dropper domains used in this campaign with intelligence from our statistical models. We convicted the domain when we saw a suspicious spike in query traffic and other dns factors. For a deeper look into the statistical models that caught this campaign and others like it, please see some presented research here by Dhia Mahjoub.



Investigate shows a spike in query traffic from a dropper/redirect domain
Allowing the MetaMorfo trojan to execute in a sandbox reveals a command and control server resolving to the following ip addresses:



Investigate shows the IP addresses associated with this command and control server
We had the following top countries requesting these malicious domains on our resolvers:

Requestor geo distribution:
Brazil , US, Canada, China, Italy, Poland, Singapore, Russia, Ireland

Conclusion

Threat actors will use what works to increase malware infections, and the current COVID-19 pandemic is no different. Although it may seem urgent given the current circumstances, it's best to treat any attachments or links received from unknown or even known individuals with

caution before clicking.

Cisco continues to track malicious campaigns themed toward COVID-19 along with the many other tactics used by cyber criminals. Our statistical models analyze over 200 billion Internet requests per day, convicting malicious infrastructure before it can be used in attack campaigns. We can also help you better protect all of your remote users with Cisco Umbrella.

To learn more, check out this blog or start a free trial today.

For up to date information on how Cisco is following the latest in malware campaigns around COVID-19 scams, please refer to the following articles:

- https://blog.talosintelligence.com/2020/03/covid-19-pandemic-threats.html
- https://blog.talosintelligence.com/2020/03/covid-19-relief-package.html
- https://support.umbrella.com/hc/en-us/articles/360041720451

IOCS:

Uris:

/upcloud4

/upcloud5

/upcloud7

/online8

/update2

Dropper/Redirects:

acalvet[.]com

acbras[.]com

arjoflor[.]com

arjoflos[.]com

bergadimspower[.]com

berkesteermaster[.]com

contatoonline1[.]com

famartil[.]com

oawyri[.]com

oawyr[.]com

parnerimcarpich[.]com

qpfhd[.]com

rjmwqf[.]com

rstmir[.]com

servicosfcporto[.]com

sirdexs[.]com

MetaMorfo C&C:

Megasena1.duckdns[.]org

IPs:

hxxp://35.192.198[.]16:80/_nomedia.tar
94.177.160[.]157
149.248.55[.]177
80.211.255[.]177

Hashes:

0461143b7daa61fc403f551a705774c4125793316a141135ffaa165a87586a52
Ff9a59d4aace29b9274029f5573f41a91b2493e7f64e976da2dff4e2298fdd44