

# SIXGILL REPORT

---

## Virus in the Wild

### Coronavirus Discourse on the Dark Web

March 1, 2020



**SIXGILL**

# Virus in the Wild

## Executive Summary

---

- The novel coronavirus (COVID-19) has captivated the attention of worldwide media, social media, and internet discourse. Many that want to discuss it on secure channels have turned to secure messaging apps, such as Telegram, QQ, and Discord, as well as deep and dark web forums.
- This report reviews quantity and quality of discourse during the period from January 15, when the news was just breaking, through February 15, when awareness of the virus had saturated international discourse.
- Worldwide, mentions began to rise significantly on January 21 until peaking on January 28, then radically declining over in the following two days until normalizing. Presumably, the initial news resulted in major excitement and activity before reverting.
- Divided by region, the most volume was in Chinese, followed by regional languages and forums, and then global. Notably, global mentions rose more gradually and peaked later. Those closer to the epicenter were the earliest and most concerned.
- Themes of discourse about COVID-19 appear to be largely informational. Most posts share and discuss news and other information, such as how to stay protected. Many posts are political, critical of governmental efforts to contain the pandemic (especially in China, where public expression of criticism is forbidden). Many more are outright conspiratorial.
- Our research noted that the quantitative patterns and the content of discourse surrounding COVID-19 on the deep and dark web does not differ categorically from what one can find on the clear web. Indeed, while we may tend to think of the dark web as an underground criminal realm, people with a variety of motivations also log in. Furthermore, we also see that even in forums dedicated to crime, the topics of discussions are sometimes concerned with general global events. Still, we did discover several attempts to monetize fears of the virus through social engineering and malware.
- Ultimately, we must understand the dark web as an ecosystem connected to the global community, influencing and being influenced by broader events.

## Introduction

Dark web activity is very often focused on computer viruses. Sometimes, however, it takes a virus of another kind—biological—to remind us of the dark web’s original intended use, as a medium for anonymous communication between individuals, unimpeded by governments and geography.

The novel coronavirus, known officially as COVID-19, that broke out in China’s Hubei province in December 2019, has captivated the attention of worldwide media, social media, and internet discourse. As the virus rapidly spreads throughout China and beyond, a global audience hungers for official news and shares unsubstantiated rumors.

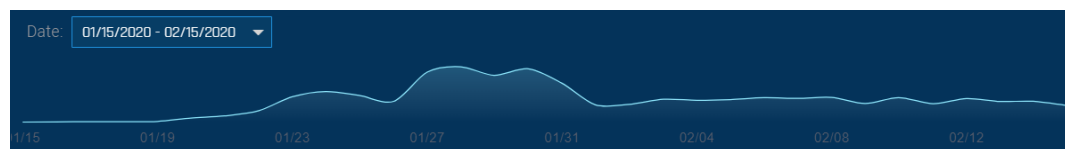
Undoubtably, many want to discuss COVID-19 on more secure channels, including those wishing to avoid Chinese state surveillance. Accordingly, we noted interesting patterns of discourse in secure messaging apps, such as Telegram, QQ, and Discord, as well as a spike in discourse on deep and dark web forums.

This report reviews the period from January 15, when the news was just breaking, through February 15, when awareness of the virus had sufficiently saturated international discourse. We will perform a quantitative and then qualitative analysis of mentions of the novel coronavirus and investigate the discourse in the following categories: Chinese language, regional languages and forums, and international languages.

## Quantity of Discourse

We searched for mentions of the virus and associated terms in English, Chinese, Russian, Japanese, Korean, and Vietnamese, between the dates January 15 - February 15.

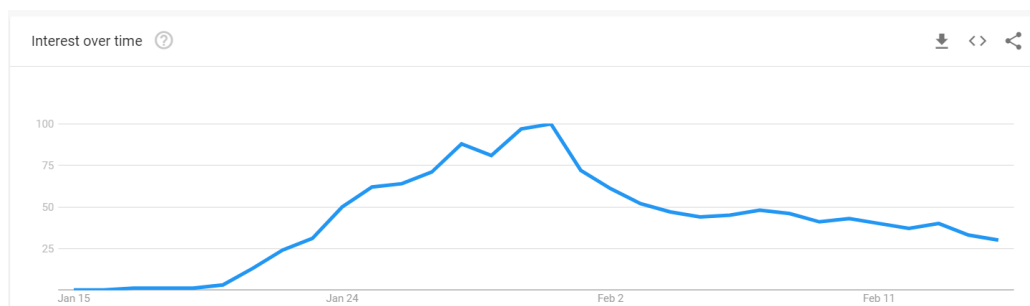
Figure 1: Total mentions of COVID-19 (and associated terms)



Over 61% of these posts were in English, followed by Chinese (34%), with Swahili at a distant third (1.3%). Singaporean forums accounts for nearly 45% of those mentions, followed by Telegram (25%) and Malaysian forums (8%).

Mentions began to rise significantly on January 21, then plateaued for a week before more than doubling from January 26 to 27. On January 28, they peaked at 12,884 posts. However, mentions radically declined in the final two days of

Figure 2: Google Trends graph of worldwide searches of "Coronavirus"



We wanted to understand how deep and dark web mentions varied based on geography. However, by design the dark web enables geographic anonymity, so instead we divided discourse by linguistic groups. This allows us to gain a better understanding of discourse in China, regional countries, and the general international community.

## CHINESE MENTIONS

In Chinese, a steep rise in mentions began on January 21 and peaked on January 28 at 8,400.

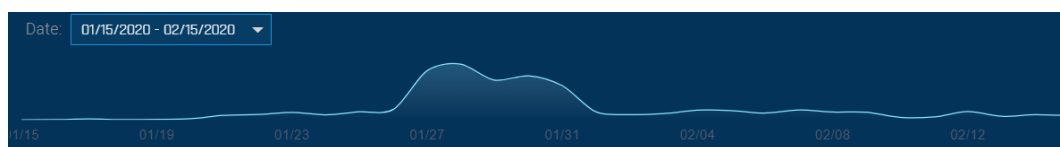


Figure 3: Chinese mentions of COVID-19 (and associated terms)

The most popular dark web forums for Chinese-language discourse were Chinese (19%) and Singaporean (1%), while Telegram (65%) and Discord (14%) led messaging platforms.

In the final two days of January, mentions of the virus in Chinese dropped nearly as steeply as they rose. Although this drop is consistent with the trend of global mentions, in China the drop was far more severe.

This drop includes a decline in activity on the Chinese messaging app QQ:

<sup>1</sup><https://trends.google.com/trends/explore?date=2020-01-15%202020-02-15&q=coronavirus>

Figure 4: Chinese mentions on QQ of COVID-19 (and associated terms)



However, the largest share of the drop in volume can be attributed to Telegram (which is officially banned in China). At the peak, Telegram accounted for over 5,000 daily mentions; however, suddenly it dropped to only a few hundred. All five leading Telegram groups mentioning the virus went nearly dark.

Figure 5: Chinese mentions on Telegram of COVID-19 (and associated terms)



We questioned if there was perhaps a broader decline in Telegram volume in China during this period, or just in posts related to the virus. We found the latter to be true. General Chinese language posts on Telegram dipped from February 2-5 but rose to an even higher volume afterwards.

Figure 6: Total Chinese discourse on Telegram

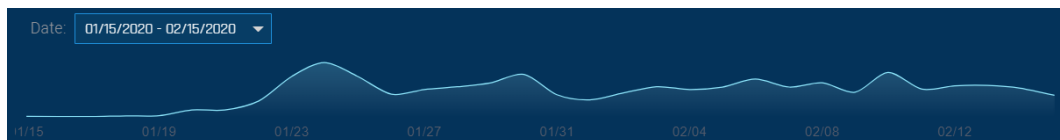


It is unclear why mentions of COVID-19 dropped so radically in Chinese-language Telegram groups, but it is notable just how sharp this is.

## REGIONAL MENTIONS

A query for mentions of the COVID-19 in regional languages (excluding Chinese) and regional forums discovered that mentions began to spike on January 20, peaked by the 24<sup>th</sup> (5,946), and then dropped slightly to a new plateau.

Figure 7: Regional mentions of COVID-19 (and associated terms)

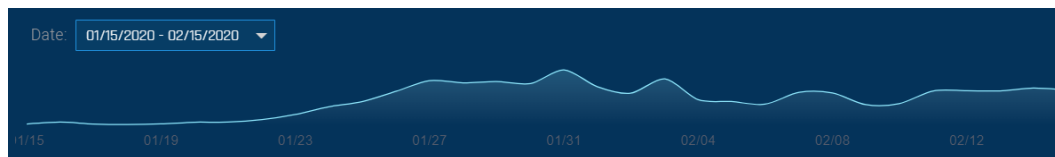


The vast majority, 83%, were on a Singaporean forum followed by a Malaysian (16%). English, one of the spoken languages of Singapore, accounted for 97% of the posts, with a few hundred in Indonesian, Japanese, and Malay.

Figure 8: Global mentions of COVID-19 (and associated terms)

## GLOBAL MENTIONS

Excluding Chinese and other regional languages and forums, a query for global mentions finds a sloping rise from January 22-27, followed by a peak on the 31<sup>st</sup> at 1,312 posts.



While Telegram displayed the most mentions at 20%, perhaps the biggest surprise is the Swahili-language forum as the leading forum at 15%. These are followed by Pastebin (12%) and a bitcoin-focused forum (11%).

Indeed, while English is the leading language of mentions (76%), it is followed by Swahili (11%), then Russian, Turkish, Spanish, and French.

Mentions in Swahili are distributed across many actors and posts. It appears that Swahili speakers are turning to the dark web for news and discussions about the virus disproportionate to other language groups.

Between the three analyzed regions, most posts were unsurprisingly in Chinese, followed by regional languages/forums, and then global. Furthermore, while Chinese and regional mentions began to spike on January 20-21 and peaked on the 28<sup>th</sup> and the 24<sup>th</sup>, respectively, global mentions rose more gradually from the 22<sup>nd</sup> until their peak on the 31<sup>st</sup>. Those closer to the epicenter were the earliest and most concerned.

## Themes of discourse

Themes of discourse about COVID-19 appear to be largely informational. Most posts share and discuss news and other information, such as how to stay protected. Many posts are political, critical of governmental efforts to contain the pandemic. As can be expected from the internet, many more are outright conspiratorial.

## CHINESE DISCOURSE

Many Chinese actors have combined an interest in the news with programming skills, such as this actor showing his visualization of the outbreak according to regional infection density.



Figure 9: A visualization of COVID-19 infections on a Chinese dark web forum

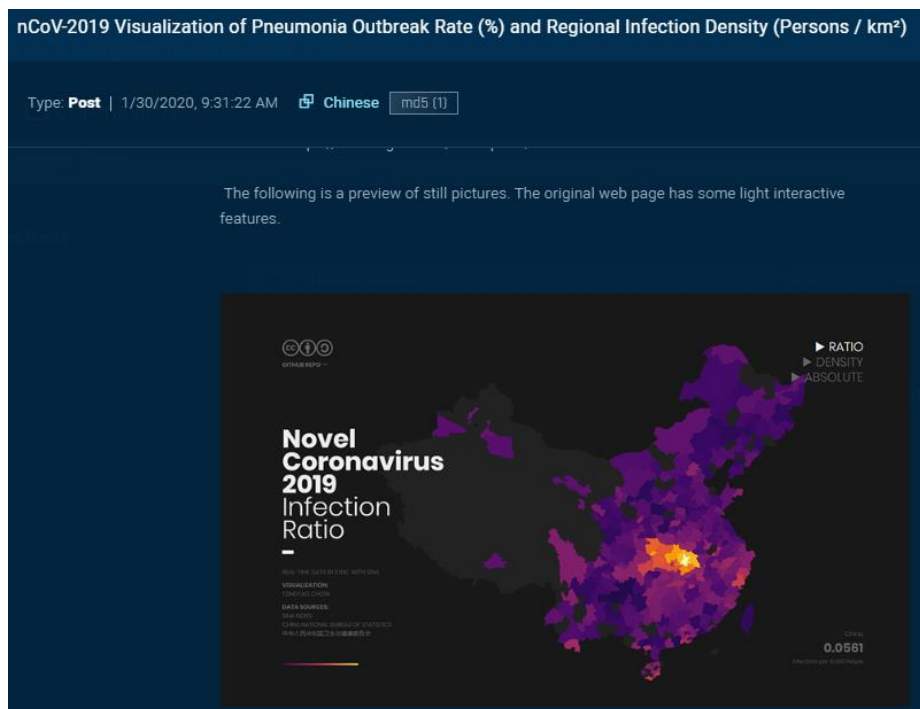


Figure 10: A discussion on Discord concerning how long quarantines will last

At the ground-zero of the virus, actors discussing COVID-19 in China frequently discuss how they have been and will continue to be affected. The following Discord discussion concerns how long quarantines will last.



Meanwhile, this Telegram group offers allegedly firsthand photos and testimony of the terrible conditions in hospitals in affected areas.

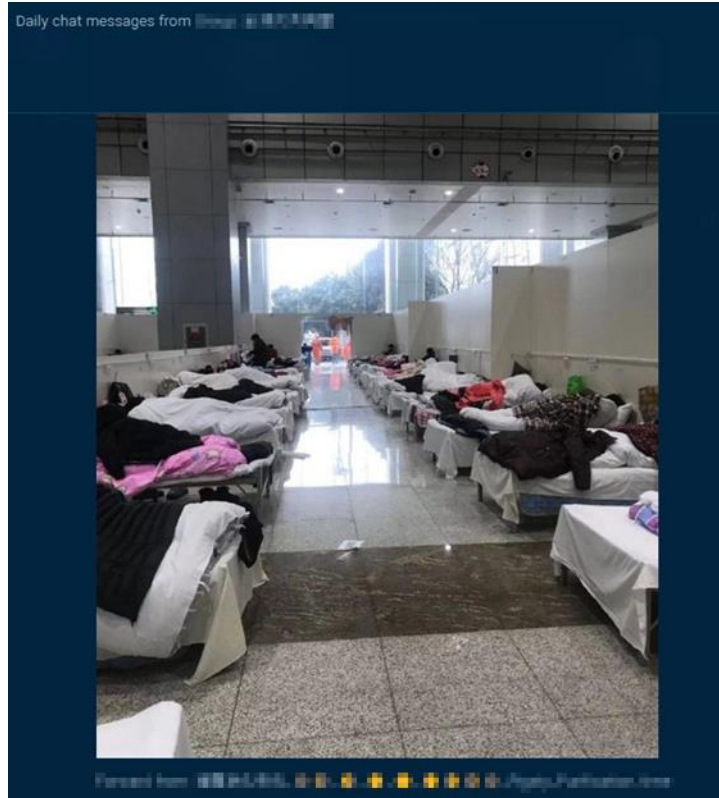


Figure 12:  
Alleged  
testimony in a  
Telegram group  
of poor  
conditions in a  
hospital in  
Wuhan's  
Quiaokou district

Forward from: Pigsty Purification News ...  
...Pigsty\_Purification, time 2020-02-06 05:48:05 Breaking news: My aunt is a newly diagnosed patient with new coronary pneumonia in Qiaokou area, At 9 pm yesterday, I was sent to a private hospital for isolation and treatment. At 3 am, I was woken up to say that I was sent to a larger hospital with better conditions. As a result, I was taken to Wuzhan Fangfang Hospital. The conditions here are very poor, which is not exactly what the news says. The electric wire was short-circuited and the power was cut off. The electric blanket could not be used, and it would be chilling at night when sleeping; One thousand people shared a toilet, and no one cleaned it. The patient's feces spilled out of the pit; I had breakfast at 10 in the morning, a few small snacks, and I did n't know if there was a landing; Dispensing medicines, limited staff, but too busy; oxygen insufficient equipment is seriously lacking, hundreds of people in the ward have no bottle of oxygen, coughing one after another. In this case the patient's condition will only worsen. 🤔🤔🤔🤔

Chinese-language dark web actors have also expressed direct criticism of the government and Chinese Communist Party (CCP). This sentiment was especially strong surrounding the death of Li Wenliang, a doctor that identified the new virus early, was allegedly silenced by local authorities, and then contracted and succumbed to the disease. The two posts below illustrate this:



Figure 13: A post in a Telegram group honoring the memory of Li Wenliang and calling for civil freedoms and the resignation of Xi Jinping

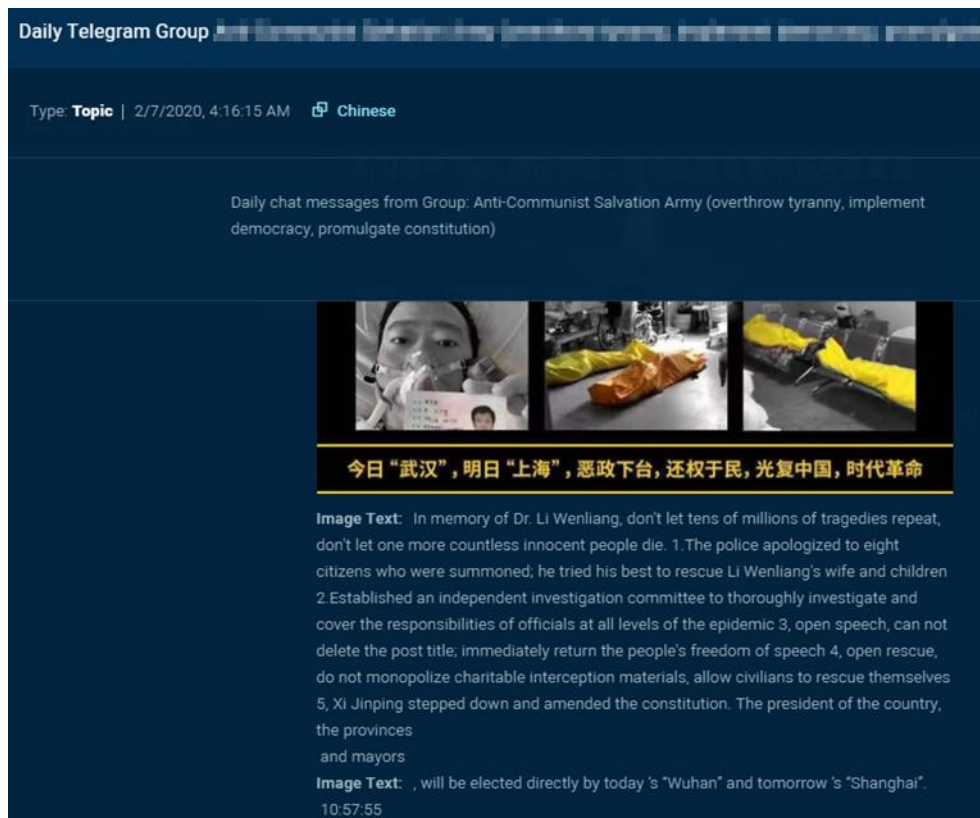
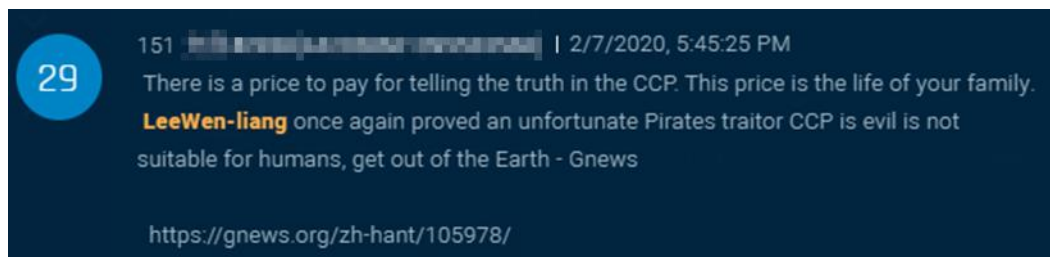


Figure 14: A post on Discord supporting Li Wenliang and criticizing the Chinese Communist Party



With Chinese state censorship of material critical of the government and party, we are not surprised to find this type of discourse on the more secure channels provided by messaging apps and the dark web.

## REGIONAL DISCOURSE

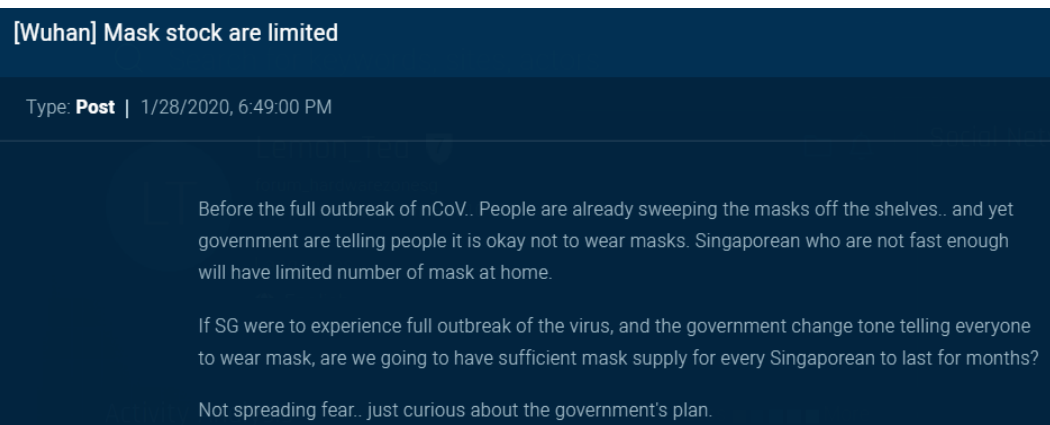
Regional discourse often mentions events in China but mostly focuses on anxiety that the virus will break out locally.

This Japanese-language post mentions a news item, that a visitor to Japan from Wuhan was diagnosed:

Figure 15: A Japanese-language post following news of infections in Japan



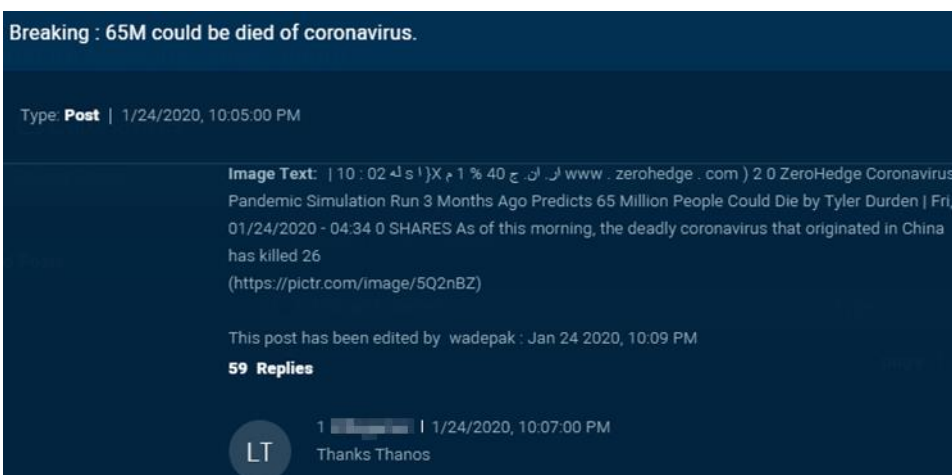
Figure 16: A Singaporean post questioning if the country is prepared for an epidemic



Furthermore, this post questions if Singapore's government has a plan to supply everyone with masks for several months.

Some actors seem far more concerned than others; one actor posted 831 times about the virus and its spread, expressing sentiment highly critical of Chinese containment efforts.

Even more alarming, this post from a Malaysian forum reports that a simulation showed that 65 million people may die from the virus.



Ultimately, people in the region are anxious to know how they may be affected.

Figure 18: A post on a bitcoin-focused forum asking how the virus will affect crypto markets

## INTERNATIONAL DISCOURSE

International discourse focuses largely on news developments. Forums centered on a certain topic speculate about how the virus will affect it. In the post below from a bitcoin-focused forum, discussions focus on the virus's impact on bitcoin prices.



Conspiracy theories spread nearly as fast as the virus itself, specifically on Pastebin, a platform for anonymous posting. The following two posts "prove" that the virus is a lab-developed bioweapon.

Figure 19: A conspiratorial paste from someone alleging to be a bioweapon expert from the Romanian Ministry of Defense

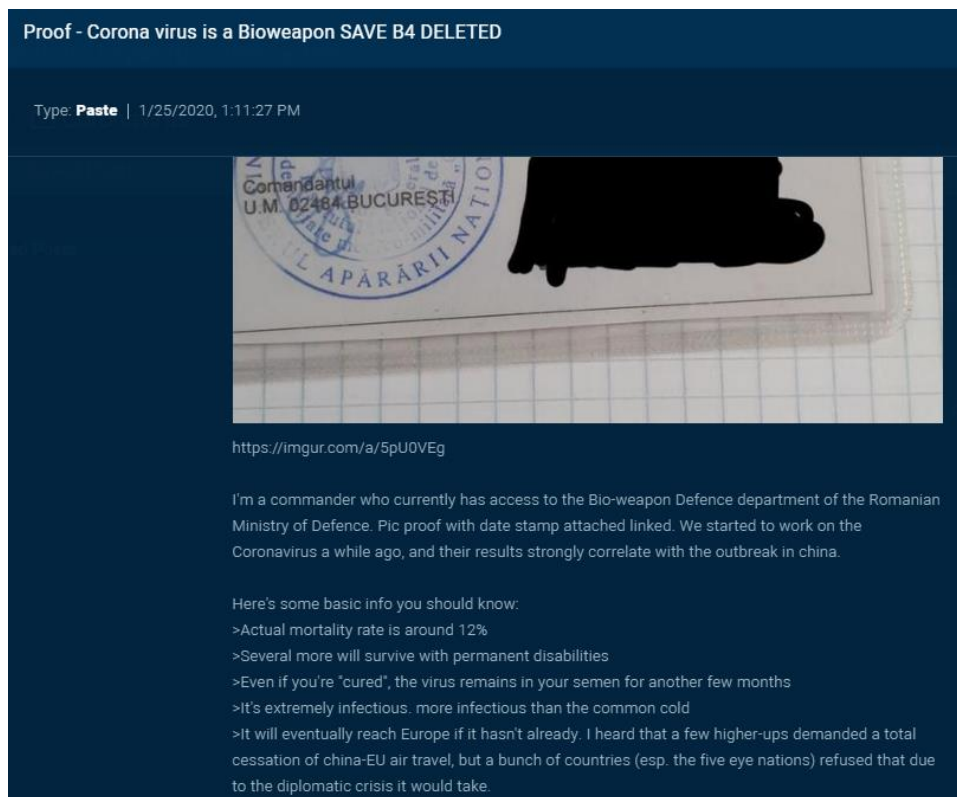
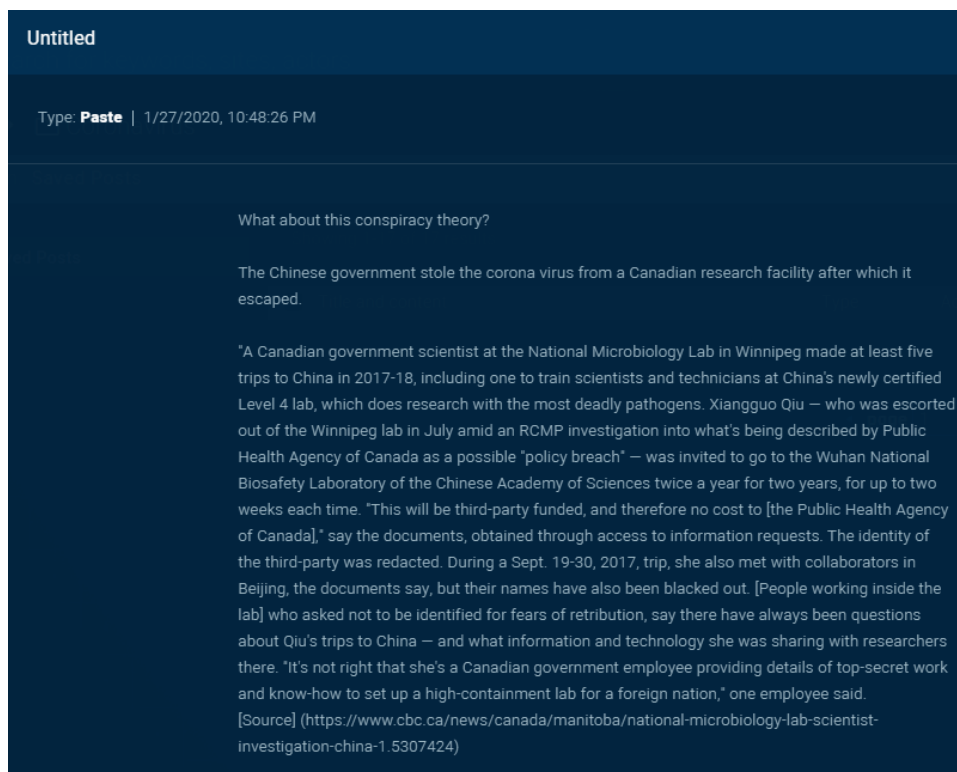


Figure 20: A conspiratorial paste alleging that the virus is a bioweapon developed by Canada and stolen by China, which subsequently escaped the lab



We discovered informational discussions of COVID-19 in forums generally dedicated to cybercrime. In this post in popular Russian-language malware forum, a threat actor asks if the virus will spread worldwide. Moreover, the actor speculates the economic impact, claiming that it will strengthen the dollar, while also conjecturing that if this event is truly apocalyptic, individuals should buy weapons and food to ensure survival.

Figure 21: A post in a popular Russian-language malware forum asking if the virus will have major economic and social impact, answered by a familiar threat actor

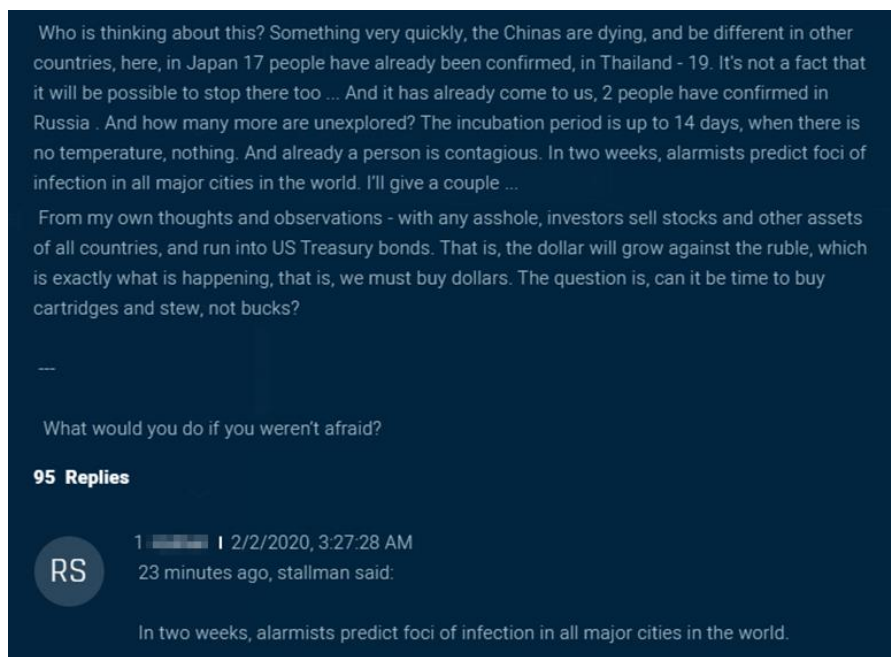


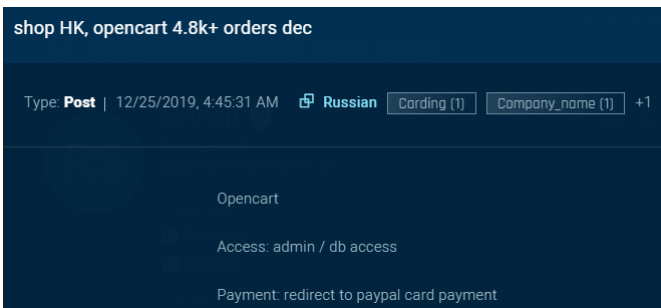
Figure 22: This actor is a known developer of credit card sniffers

This post, and several others about COVID-19, is answered by the same actor that we analyzed in our report on credit card sniffers.



Figure 23: A post from this actor selling access to a Hong Kong e-commerce database

Apparently, this actor is quite busy, worrying about the virus from China while deploying his own viruses against e-commerce stores in Hong Kong. It

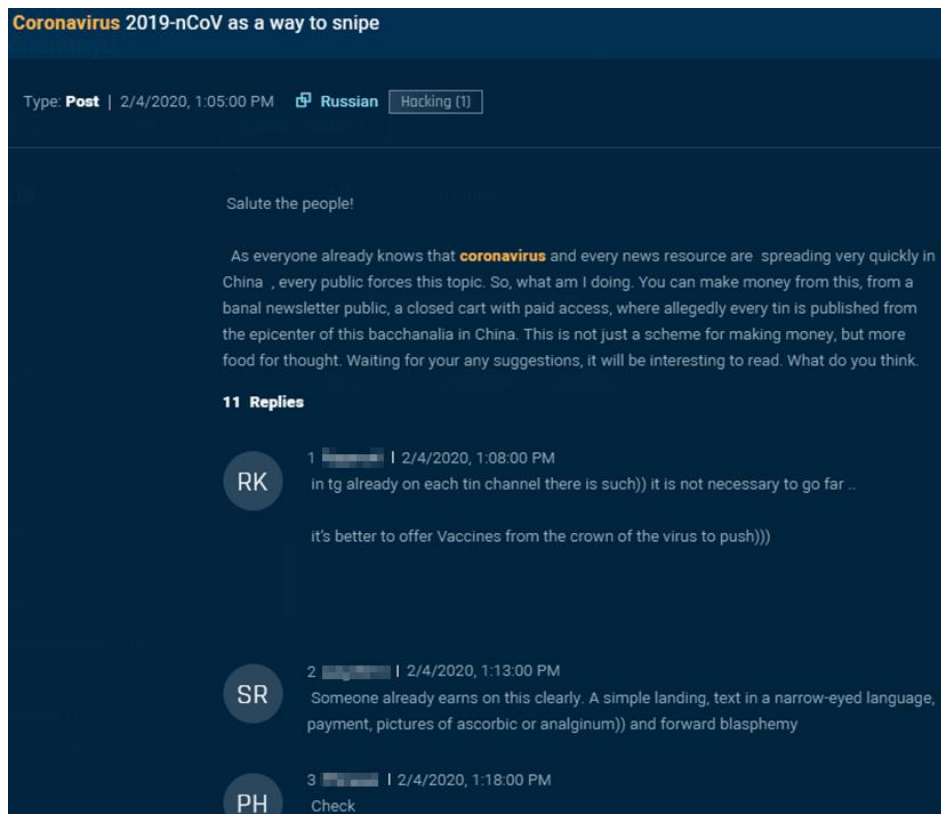


seems like this virus is on everybody's mind, regardless of who and where.

Finally, we did identify discussions of how to perform social engineering and malware attacks in order to profit from individuals afraid of infection.

The post below from a different Russian-language forum suggests publishing a newsletter about developments, luring users to pay for fake exclusive information.

Figure 24: A post suggesting a method for a social engineering to profit from fears of the virus





Even more nefarious, the post below from a different Russian-language cybercrime forum sells a virus profiting from the virus: for \$700, one can buy a weaponized version of the popular map from Johns Hopkins Center for Systems Science and Engineering (CSSE). When opened, a payload is executed, compromising the host system. From there, the attacker may steal data, control the system remotely, and propagate the virus onwards.


Figure 25: A post selling for \$700 a malicious version of a popular virus-tracking map, which can be used to compromise a victim's machine

[ПРОДАЖА] 📢 New Exploit and Corona Virus Phishing Method!

Type: **Post** | 2/23/2020, 1:45:34 AM 🌐 **Russian** Malware (2) Email\_address (1) +3

New Exploit and Corona Virus Map Phishing method

New Exploit Plus Crown Virus Distribution Card Wiring



**Image Text:** Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE Larta T :: lal Cariliurm :! la kacead 75,161 2,008 14,356 2 'desthe Hutini Mairln: china 9.128 HIXHI HI Ilubaltainlend China Cmlrlrmd Cннк 1у Countryltoglon \* y dectha L6s recovcrod Tii XSS.is Heran ainlerel 74,148 Mainland China Guangelong Mairl

The preloader loads the map and the .jar loader which can contain the payload or load it from the outside.

PreLoader size less than 1Kb and it does not need crypting !!!

Does not trigger UAC and Bypass Windows Defender !!! see demo video.

Thus Loader is always FUD and you can mail it as attachment safely.

The preloader size is less than 1Kb and it does not need to be crypted !!!

Does not call UAC and bypass Windows Defender !!! Look at the demo video.

The preloader is always FUD and can be easily distributed in bulk.

Price \$ 200 for private build + your Java CodeSign certificate.

With my CodeSign certificate price is \$ 700

jabber: freebeer@404.city (mailto: freebeer@404.city) (OTR)

Beware of scammers. Alway confirm deal in PM!

Escrow (guarantor) is welcome on your expenses

## Conclusion

---

This paper surveyed discourse about COVID-19 in Chinese, regional countries, and in international discourse. With the exception of China, where official internet censorship pushes anti-government sentiment underground, the discussions of the virus on the dark web appear to reflect both in quantity and in quality what we would expect to find on the clear web.

We may tend to think of the dark web as an underground realm inhabited exclusively by criminals. However, in reality, users with non-criminal intent also log in, motivated by a desire to communicate anonymously and to gain and share knowledge. This is especially true in places where the clear web is monitored or blocked.

We also see that criminal spaces in the dark web do not occur in a vacuum. Even in forums dedicated to crime, the topics of discussions are sometimes concerned with general global events. Furthermore, not all threat actors are engaging in malicious activity all the time; individuals are multidimensional and discuss topics of general interest. Still, we did find examples of criminal activity surrounding the virus, as malicious actors attempt to profit from widespread fear.

Ultimately, we must understand the dark web as an extension of the clear web. It is a community connected to the broader global community. In order to perform their tasks more effectively, intelligence analysts must remember that there is a full persona behind the actor name. Only through holistic analysis of this ecosystem can one understand the broader developments in the threat landscape.