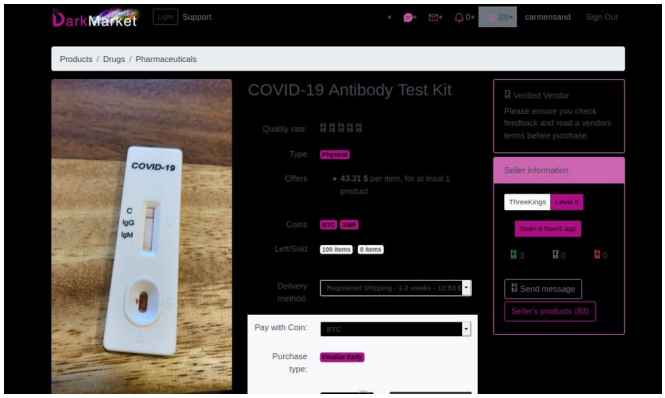
Sketchy darknet websites are taking advantage of the COVID-19 pandemic – buyer beware

19 August 2020, by David Maimon



If it's an in-demand COVID-19 commodity, chances are it's available on darknet markets. Credit: David Maimon, CC BY-ND

Underground markets that sell illegal commodities like drugs, counterfeit currency and fake documentation tend to flourish in times of crisis, and the COVID-19 pandemic is no exception. The online underground economy has responded to the current crisis by exploiting demand for COVID-19-related commodities.

Today, some of the most vibrant underground economies exist in darknet markets. These are internet websites that look like ordinary e-commerce websites but are accessible only using special browsers or authorization codes. Vendors of illegal commodities have also formed dedicated group-chats and channels on encrypted instant messaging services like WhatsApp, Telegram and ICQ.

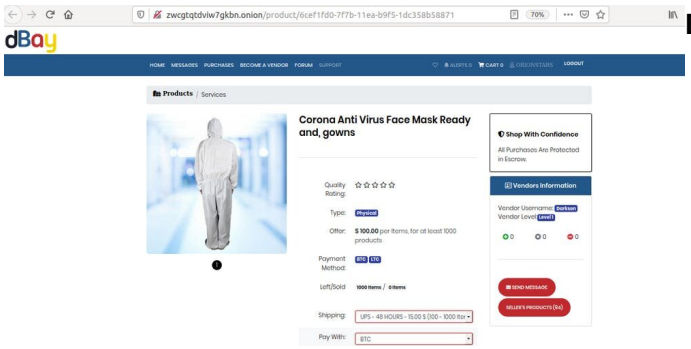
The Darknet Analysis project at the Evidence-Based Cybersecurity Research Group here at Georgia State University collects data weekly from 60 underground darknet markets and forums. My colleagues Yubao Wu, Robert Harisson and I have analyzed this data and found that three major types of COVID-19 offerings have emerged on darknet markets since late February: protective gear, medications and services that help people commit fraud.

Using these darknet markets is risky business. First, there's the built-in risk of becoming the victim of a scam or buying counterfeit products when purchasing products from underground vendors. There are also health and legal risks. Inadvertently buying ineffective COVID-19 protective gear and dangerous remedies from unregulated sellers could physically harm buyers. And purchasing information and services with the aim to defraud people and the government is a criminal offense that carries legal penalties.

Personal protective equipment

Several vendors have added protective gear such as face masks, protective gowns, COVID-19 test kits, thermometers and hand sanitizer to their list of products for sale. The effectiveness of this protective gear is questionable. Underground vendors typically do not disclose their products' sources, leaving consumers with no way to judge the products.

One example of the uncertainties that surround protective gear effectiveness comes from one of the encrypted channel platforms we monitored during the first few days of the pandemic. Vendors on the channel offered facemasks for sale. Demand for facemasks was very high at that time, and people around the world were scrambling to find facemasks for personal use.



COVID-19 protective gear is a common product type on darknet e-commerce sites. Credit: David Maimon, CC BY-ND

While governments and suppliers faced difficulties in meeting demand for facemasks, several vendors on these platforms posted ads offering large quantities of facemasks. One vendor even uploaded a video showing many boxes of facemasks in storage.

Given the global shortage of facemasks at the time, our research team found it difficult to understand how this vendor in Thailand could offer so many for sale. One disturbing possibility is that they sold used facemasks. Indeed, authorities in Thailand broke up an operation that washed, ironed and boxed used facemasks and supplied them to underground markets.

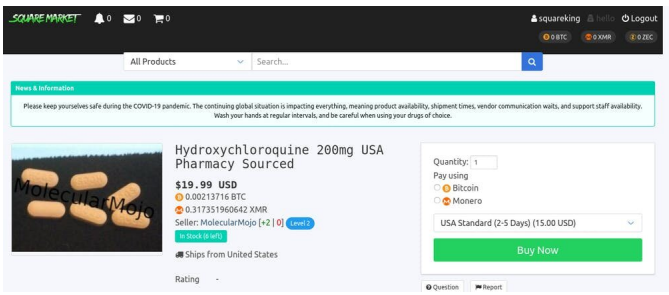
Treatments

Darknet vendors are also selling medications and cures, including effective treatments, like Remdesivir, and ineffective treatments, like Hydroxychloroquine. They're are also selling various purported COVID-19 antidotes and serums. Some vendors even offer to sell and ship oxygen ventilators.

Using COVID-19 medications purchased on darknet platforms could be dangerous. Uncertainties about the true identity of medication manufacturers and the ingredients of other cures leaves patients vulnerable to a wide array of potentially detrimental side effects.

DIY fraud

Government efforts to relieve the financial stress on individuals and businesses from the economic impact of the pandemic has led to a third category of products on these markets. We have observed many vendors offering to sell online fraud services that promise to improve customers' financial circumstances during this crisis.



Darknet markets offer ineffective and potentially dangerous COVID-19 therapies, including hydroxychloroquine, which studies have shown is not an effective treatment. Credit: David Maimon, CC BY-ND

These vendors offer to either support customers in putting together fake websites that allow them to lure victims into disclosing their personal information, or simply provide stolen personal information. The stolen information can be used to file for unemployment benefits or obtain loans. Some vendors go a step further and offer support in the fraudulent benefits application process.

COVID-19-related fraud could have grave consequences for individuals whose identities have been stolen and used to apply for government benefits or loans, including the loss of future government assistance and damage to credit scores. Fraudulent requests for COVID-19 relief funds filed using stolen personal information also puts additional strain on federal, state and local governments.

Digging up the data

The size of the online illicit market of COVID-19

essentials is unknown. We aim to collect enough data to provide an empirical assessment of this underground economy.

There are several challenges to understanding the scope of the COVID-19 underground market, including measuring the magnitude of the demand, the extent supply meets that demand and the impact of this underground economy on the legitimate market. The unknown validity of darknet customers' and vendors' reports about the products they purchased and sold also makes it difficult to assess the underground market.

Our systematic research approach should allow us to overcome these issues and collect this data, which could reveal how online underground markets adjust to a worldwide health crisis. This information, in turn, could help authorities develop strategies for disrupting their activities.

Provided by The Conversation
APA citation: Sketchy darknet websites are taking advantage of the COVID-19 pandemic – buyer beware (2020, August 19) retrieved 2 December 2021 from https://techxplore.com/news/2020-08-sketchy-darknet-websites-advantage-covid-.html