Cybercriminals cash in on black market vaccine schemes

intel471.com/blog/fake-covid-vaccination-cards-cybercrime

If you look back through all of the research Intel 471 has released on cybercriminals making money on stolen digital assets, a major takeaway is that the cyber underground will adopt any scheme, as long as it results in money being made. With the world trying to move past the global COVID-19 pandemic, another opportunity for illegal gains has struck.

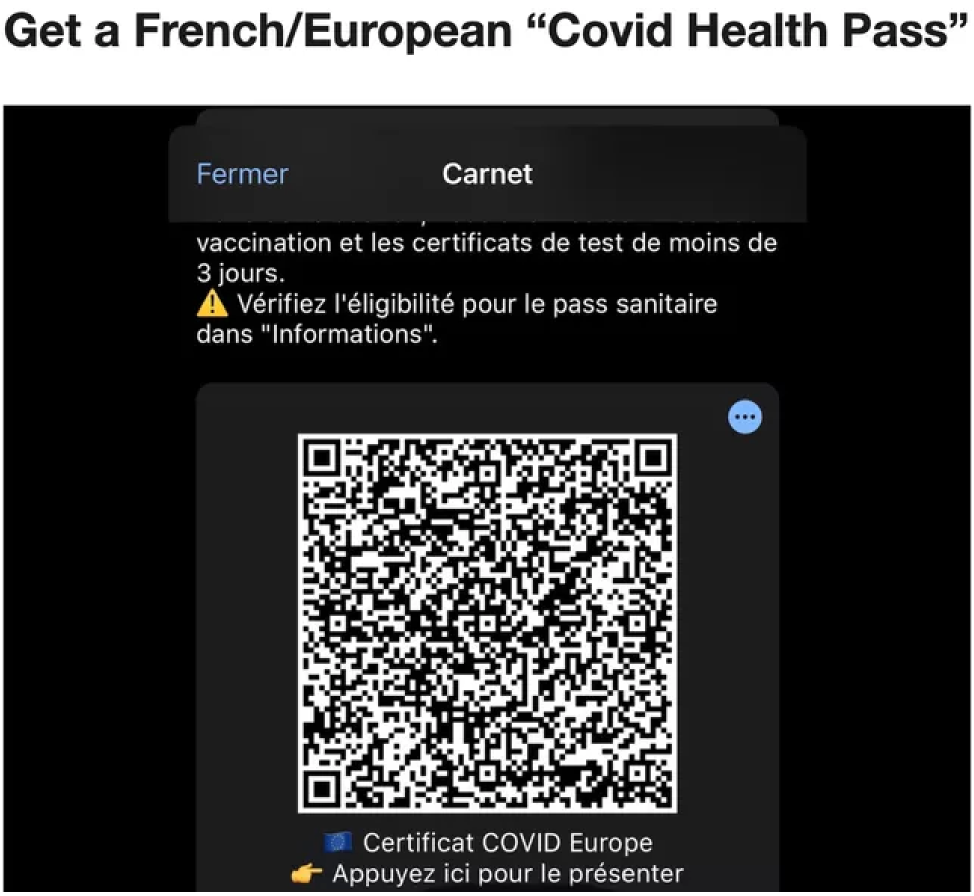
Intel 471 has observed numerous actors on various underground forums selling fake COVID vaccine certifications, as well as several forums hosting advertisements for COVID-19 vaccines. While these advertisements have proliferated for months, we have observed these schemes growing on underground forums that are rooted in the cybercrime ecosystem.

Of those fake vaccine passes being advertised, we have seen the concentration placed on the United States' Centers for Disease Control and Prevention's vaccination card, which is a paper form, and the European Union's vaccine passport, which is issued in both digital and paper forms. On one particular cybercrime forum, an actor has listed several advertisements for fake vaccination cards that parrots a lot of the misinformation that surround the various COVID-19 vaccines.

"We do this to help people who are in critical situations and want to travel urgently," the advertisement reads. "Watch out and stay away from the vaccine; it's poisonous. Kindly pass out the message to those who are still blind out there, so many secrets are hidden from us. The minority ruling are trying to destroy mankind."

The actor has set up several communication channels for anyone interested: potential customers can reach out via encrypted messaging services Telegram, WhatsApp, and Wickr, or encrypted email service ProtonMail.

Another advertisement on the same forum offers fake CDC cards. These falsified documents are focused on the European and French documents and associated false QR codes. The website, accessible via the TOR browser, shows what the final QR code product will look like:


Get a French/European “Covid Health Pass”

vaccination et les certificats de test de moins de 3 jours.
⚠️ Vérifiez l'éligibilité pour le pass sanitaire dans "Informations".

🇪🇺 Certificat COVID Europe
👉 Appuyez ici pour le présenter

An example of a fake French digital COVID passport taken from an underground website. (Intel 471)

With regards to the actual vaccine, an actor’s advertisement that Intel 471 observed claimed to be able to send potential buyers numerous different vaccines currently on the market: AstraZeneca, Johnson & Johnson, Moderna, Pfizer, and Sputnik V. Buyers were then directed to visit a particular website set up for sales. However, that e-commerce website was not working at the time this blog post was published.

There have been numerous reports that this falsified document practice has been going on for months. However, we have seen the market change as the virus causes different issues in various parts of the world. Actors will:

- Read open-source news to determine which countries are not getting enough, or any, deliveries of the vaccine.
- Market the illegal vaccine to these developing countries since these nations have no private way of obtaining vaccines and must instead rely on COVAX distribution.
- Undermine the pharmaceutical companies’ efforts to distribute the vaccine, putting people in danger since they have very little recourse to determine if the vaccines are legitimate.

Be it underground vaccine sales or counterfeit vaccine passes, actors are monetizing the fear and misinformation around COVID-19, creating a new market that has been constructed partly by pushing people who have never purchased anything illicit to buy things off of the underground. While the schemes carried out in this blog do not directly impact an organization’s cybersecurity defenses, it can hurt pharmaceutical companies by robbing them of consumers and damaging their brand reputations. In addition, fake vaccine passports harm healthcare, erodes government trust with false information, and can disrupt local and national economies.

No matter the damage wrought, it shows that cybercriminals and the forums where they gather online will take on any scheme, no matter how technical, in order to make money.