CryCryptor, ransomware masquerading as a fake COVID-19 tracking app, is spreading across Canada and encrypting data on Android devices. This new threat is mostly targeting the victim's pictures, videos, and documents in addition to other user data. After a file is encrypted, the original is deleted and a "readme_now.txt" is created instructing the user to send an email with a personalized ID. The developers responsible have tried to hide the true nature of the project by submitting it to the VirusTotal service for verification. Thankfully, a decryption tool has been created that exploits the encryption key being stored in the shared preferences and the service being unrestricted. Although the program claims to be for research purposes, it's clear this isn't true since the malware is easy to use. There is another similar strain of malware that was released in May pretending to be Italy's official coronavirus-tracking app ahead of their real app.

Although this malware is easy to remove, it emphasizes how the victim should pay close attention to the permissions of each app on their device. It should have been a huge red flag for an app of this nature to be requesting access to their personal files.

https://threatpost.com/emerging-ransomware-photos-videos-android/156893/

https://www.tripwire.com/state-of-security/security-data-protection/new-crycryptor-ransomware-masqueraded-as-covid-19-tracing-app/

https://www.welivesecurity.com/2020/06/24/new-ransomware-uses-covid19-tracing-guise-target-canada-eset-decryptor/