CERT-PH COVID-19 Cyber Related Feed

Period Covered	**April 23, 2020**
Issue Date	**April 24, 2020**
TLP:WHITE	

Summary

The latest cyber threat topics gathered from the web and analyzed by the CERT-PH research team over the last 24 hours that may impact the Philippine government and cyberspace:

- **University of Washington and Microsoft COVID-19 Application**
- **COVID-19 Tracing Apps Have to Go Viral to Work**
- **Domain Registrars Under Pressure to Combat COVID-19-Related Scams**

Description

University of Washington and Microsoft COVID-19 Application

2020.04.23| Source(s): GeekWire, Seattle Pi

Analysis:

In partnership with Microsoft, the University of Washington has launched a new contact tracing application that will be used to monitor and track the spread of the COVID-19 pandemic. CovidSafe is a mobile application available for both android and iOS users which will make use of the exchange of Bluetooth signal of smartphones where it will log other application users within a limited proximity. It only uses a fixed random number that will be sent to other application users that will serve as their identification to protect the anonymity of the user. Once a user is confirmed positive, the ID number will be given that will be used to search and notify those who have contacted the user. The data logs and collections will be locally stored on the user's device and will only be reviewed once a user tested positive for the disease. In addition the application is open source and does not use any third party application for data management and collection.

COVID-19 Tracing Apps Have to Go Viral to Work

2020.04.23| Source(s): Coindesk

Analysis:

Different Software companies and government bodies around the world started to create their own contact tracing application that can be used in their fight against the pandemic but for it to be successful, it must be regularly used by individuals and be downloaded by many. While this kind of technology will greatly help in conducting contact tracing on possible contraction of the disease, it also stirs a lot of privacy and security issues with experts and public alike. Data collection and management from its users is hardly important as its features and capabilities. Misuse of user's collected data has been feared by many as it can be used by unknown malicious actors or even its own nation to conduct surveillance and monitoring on its own citizens. This fear and anxiety led people to disregard the benefits and assistance these kinds of applications can give to their government and even medical personnel who conduct tracing. Another reason is that the application being voluntary means people can just ignore its government call and do not use the application.

Domain Registrars Under Pressure to Combat COVID-19-Related Scams

2020.04.23 | Source(s): Dark Reading

Analysis:

U.S Lawmakers are seeking information from domain name registrar and web hosting services on what they are doing to combat the current spike in the registration of malicious websites that hosts COVID-19-related scams and malicious intents. The letter seeks answers from the companies on what actions they have taken to addressed the current situation where many fake and malicious domains have appeared that uses COVID-19 schemes and other in-demand services such as video conferencing and media entertainment service, and what steps they will take to further prevent these hackers from creating and registering websites that will be used for their malicious intents. One has responded that they have stopped automated registration of sites containing names that include "coronavirus," "COVID," and "vaccine.", while the other implements rapid responses to incoming complaints, regular cooperation with law enforcement, and internal systems and processes that proactively identify illegal content. Email phishing was also prevalent since many people fell for these fraudulent tactics. According to a security company, COVID-19–based phishing lures have been far more successful than other bait in terms of getting people to open malicious attachments or follow links to malicious sites as people want to be informed about the latest development around them and to other places. Through the actions and steps taken by these companies to address these issues, cybercriminals may need to take added measures to carry out their malicious operations.

CYBERSECURITY BUREAU
Address: 49 Don A. Roces, Diliman, Quezon City
Phone: +63(2) 8920 0101 local 1708
Email: cert-ph@dict.gov.ph
Web: https://www.ncert.gov.ph/