

CERT-PH COVID-19 Cyber Related Feed

| | |
|------------------|-------------------|
| Period Covered | April 24-26, 2020 |
| Issue Date | April 27, 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:

- [Contact Tracing Application Maybe Exploited via Bluetooth Vulnerabilities](#)
- [Apple and Google Accelerates Coronavirus Contact Tracing Apps Plan](#)
- [Apple Refuses to Comply to UK, France, and Germany's Demands](#)
- [Australia Launches Controversial COVID-19 Tracking Application](#)

Description

Contact Tracing Application Maybe Exploited via Bluetooth Vulnerabilities

2020.04.26 | Source(s): ZDNet

Analysis:

Android smartphones running on version 6.0 or earlier were prone to security vulnerabilities since these devices are not receiving security updates and patches. According to Google's data as of 2019, 40% of android users around the world use version 6.0 or earlier. Since earlier versions of Android are still in the market and are much cheaper relative to latest releases, it appeals more to the low budget individual than its successors. This is alarming since contact tracing applications utilize the Bluetooth technology and some anonymous hackers can also exploit these technologies to gather data on users. The exploitable vulnerabilities can allow remote attackers to run arbitrary code execution on affected Android devices and to gather data on other users within the vicinity. As of now there are significant increases in attackers targeting the bluetooth technology, but rather the applications that use Bluetooth are more prone to such attacks. With a different application being developed that conducts contact tracing capabilities, it open new ways for an attacker to compromise other devices and harvest user's data.

Apple and Google Accelerates Coronavirus Contact Tracing Apps Plan

2020.04.24 | Source(s): BBC, Tech Crunch

Analysis:

Google has updated their technical details of the contact tracing system they are planning to release together with Apple, saying new features would strengthen privacy protections and give health authorities more detailed data. The technology they are developing does not employ GPS location data and stores most sensitive data in a decentralized way, on users' phones. With iOS, applications that transfer Bluetooth data on the background are disabled, which means iOS devices must be unlocked that will drain its battery faster. Thus, only the API being developed has the ability to bypass this restriction. Apple and Google's system is similarly based on the use of Bluetooth technology, where the exchange of a pseudorandom number via Bluetooth electronic signal will be used to log matches without revealing the users' names, location or other identifying information. The companies also tried to address health researchers' concern over its effectiveness since Bluetooth signals can penetrate some walls and produce false-positive results. To accommodate this issue, the data provided will have the Bluetooth power levels

to better estimate how close two phones came to each other and for how long , letting authorities set their own thresholds for when to alert people. Lastly, it will also include the timeline of the data that determine how many days have passed since the last contact to help authorities notify users about what steps to take.

Apple Refuses to Comply to UK, France, and Germany's Demands

2020.04.24 | Source(s): Business Insider, Apple Insider

Analysis:

It seems that Apple stands firm in its advocacy to promote decentralization and limit the data gathered from contact tracing applications from its users. This has been a problem to different countries since their developed contact tracing app heavily relies on these factors. On iOS, applications that transfer data over Bluetooth are prevented from running in the background to protect user's data, which severely impacts the operating capabilities of contact tracing apps that typically need to run continuously in order to be effective. Another issue is how to handle the user's data, while Apple and Google are requiring the application to handle the user's data in a decentralized manner, with no information leaving the user's device until they are positive in COVID-19 diagnosis. However, France, Germany, and the UK's NHS wanted to store the gathered data in a central server. The solution to this is through the use of the Apple-Google API, as it will bypass the Bluetooth-scanning restriction on iOS for contact-tracing apps. However, it will only be available to application developers who obey and implement the standards they have set.

Australia Launches Controversial COVID-19 Tracking Application

2020.04.26 | Source(s): Engadget, Reuters, The Guardian

Analysis:

Australia has launched its own contact tracing application but privacy issues arise. COVIDSafe was based from Singapore's 'TraceTogether' that uses Bluetooth technology to conduct contact tracing but it stores the collected data to the user's phone and to a central server. The Australian government however, promised that the collected data will only be available to authorized health officials after an infected person has given the consent. The collected data includes names, phone numbers and postcodes, that may be used or abused by unknown adversaries. The government has also promised to delete the collected information once the pandemic has ended and it is no longer needed. Through the use of contact tracing application, it can be vital to monitor and oversee the spread of the disease and slowly restrict its transmission, and will lead to the end of the pandemic. The challenges are getting enough people to use the application regularly and garner the public's assurance over data privacy and security.

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/>