New Android Coronavirus Malware Threat Exposed: Here's What You Must Not Do

https://www.forbes.com/sites/zakdoffman/#2500618a702c

Here we go again—another warning that installing random coronavirus related apps onto your phone is fraught with risk. We have now seen multiple stories about these apps—mostly the threat is more a nuisance than a nightmare. Spamming your contacts, conducting ad-fraud on your phone to drive revenue for the malware's operators, attempted ransomware tricks that are easily fixed. But don't assume this is as bad as it gets—if you download one of these apps, you can get badly stung.

This is the message from the researchers at Check Point, with a new report into "malicious applications, masquerading as innocuous coronavirus apps, designed to take control of your Android device." And when it comes to mobile malware, that's about as serious as it gets. According to the research team, the threat hidden with these apps enables hackers to take "intrusive control of your device via a remote shell, accessing calls, SMS, calendar, files, contacts, microphone and the camera."

The good news is that these apps have not found their way onto the Play Store, but can be downloaded directly from coronavirus-related domains, luring people with the promise of information, advice, stats and trackers. By now you will have read plenty of reports into the surge of coronavirus-themed cybersecurity risks now targeting our inboxes, browsers and smartphones. The stats are stunning—51,000 virus-related domains registered since the pandemic, of which 9% are "suspicious and under investigation," according to Check Point.

According to a new Microsoft report, it's not the level of threat that has increased—they haven't noticed a huge upswing in attacks, "instead [attackers] are pivoting their existing infrastructure, like ransomware, phishing, and other malware delivery tools, to include COVID-19 keywords that get us to click." And the goal of such attacks is no different to what we faced before, "to infiltrate our inboxes, steal our credentials, share malicious links with coworkers across collaboration tools, and lie in wait to steal information that will give them the biggest payout."

This is certainly consistent with this latest warning from Check Point. "Skilled threat actors," the firm's research team explains, "are exploiting concerns about coronavirus to spread mobile malware, including Mobile Remote Access Trojans (MRATs), Banker Trojans, and Premium Dialers, via apps which claim to offer coronavirus-related information and help."

Reference:

https://www.forbes.com/sites/zakdoffman/2020/04/09/why-android-users-must-now-dodge-this-simple-15-minute-coronavirus-malware-threat/#48aeb2744c1d