Speaking of outdated software and ransomwares, researchers at the security firm Palo Alto Networks recently [discovered](http://researchcenter.paloaltonetworks.com/2016/02/new-android-trojan-xbot-phishes-credit-cards-and-bank-accounts-encrypts-devices-for-ransom/#more-12209) a new Trojan called “Xbot” that can, among other things, lock down the user’s files in the external storage, forcing them to pay US$100 through a spoofed PayPal-like site. This will most likely steal their payment information for even bigger losses, besides the $100. Xbot is primarily starting to affect phones running Android versions prior to 5.0 especially in the Russian and Australian regions.

Besides acting as a ransomware, Xbot is also a phishing malware, redirecting the phone to show its own fake UI for certain apps, instead of running the actual apps. This is being used for phishing user’s payment information, as the faked interfaces include Google Play’s payment page, and seven major Australian banks’ Android apps. It accomplishes this by first hijacking the intent data when Android is trying to change activities through a vulnerability called [“Activity Hijacking”](https://www.eecs.berkeley.edu/~daw/papers/intents-mobisys11.pdf), first discussed by Chin, et al. at the University of California, Berkeley. Once it finds the target activity, it then communicates with its own command-and-control server to supply a webpage equivalent of that view via [WebView](http://developer.android.com/intl/zh-tw/reference/android/webkit/WebView.html) which is then used for phishing. However, the researchers report that Android 5.0+ includes protection mechanisms against Activity Hijacking.

Though users running Android 5.0+ are safe from some of the malicious behaviours requiring Activity Hijacking, all versions are vulnerable to at least some of its capabilities such as phone lockdown and ransoming, or scraping sensitive data. The researchers report that the developers of this malware seem to working fast towards making it even more complex and harder to detect, and it is expected that its ability to infect phones will only increase. They have not been able to find its spreading mechanism, besides some websites where the APK is being hosted. The reported architecture of the malware is pretty flexible to support more fake UIs in the future, suggesting that the affected regions might expand from just Australia and Russia. It can then become an even more serious issue considering the number of phones running Android, especially the older versions.