How does Ghimob bypass the security measures implemented by financial institutions?

According to the article "**Ghimob: a Tétrade threat actor moves to infect mobile devices"**[1] the author describes to the reader how Ghimob by passes the security measure implemented from the financial institutions " Once infection is completed, the hacker can access the infected device remotely, completing the fraudulent transaction with the victim's smartphone, so as to avoid machine identification, security measures implemented by financial institutions and all their anti fraud behavioral systems." this shows that you might think you're protected but once you're infected everything is at risk of being stolen

Why does the trojan abuse Accessibility Mode?
The author states "Once installed on the phone, the app will abuse Accessibility Mode to gain persistence, disable manual uninstallation and allow the banking trojan to capture data, manipulate screen content and provide full remote control." this allows the Attacker to do every action smoothly

How are victims lured into installing the malicious file?
The victims are believing that the URLs or the APK files they are downloading are from the actual legit provider but are not knowing that it's a trojan horse.

What happens once the infection is completed?
The author describes what happens when the infection is completed "Once installation is completed, Ghimob tries to hide its presence by hiding the icon from the app drawer. The malware will decrypt a list of hardcoded C2 providers from its configuration file and contact each in order to receive the real C2 address, a technique we call fallback channels. " after it hides itself it will start to do recon and then start the attack

What can be done to mitigate the risk of infection
One way the author provides help to mitigate attacks for financial institutions are"
Financial institutions watch these threats closely, while improving their authentication processes, boosting anti-fraud technology and threat intel data, and trying to understand and mitigate all of the risks that this new mobile RAT family poses."

[1] Original article at https://securelist.com/ghimob-tetrade-threat-mobile-devices/99228