É possível observar que o ficheiro é maligno, tendo várias advertências de que existe um vírus Cavalo de Troia (Trojan). É possível assumir que se trata de uma aplicação utilizada para obter informações sobre o estado do tempo, dado o nome da main Activity “WeatherApp”.

O APK em questão pode ser potencialmente perigoso, dado que permite o acesso a diversas operações realizadas no dispositivo, como gerir as mensagens (“android.permission.READ_SMS”, “android.permission.RECEIVE_SMS” e “android.permission.SEND_SMS”), aceder à câmara (“android.permission.CAMERA”) ou obter informações sobre o estado do dispositivo (“android.permission.READ_PHONE_STATE”). Tem ainda acesso às operações sobre a rede efetuadas (“android.permission.INTERNET”).

Está configurada para iniciar com o arranque do sistema operativo, não sendo necessário que o utilizador dê a ordem de execução, dada a existência do Intent “android.intent.action.BOOT_COMPLETED”).

Existem diversos pedidos que são realizados através da aplicação. No entanto, existem alguns endpoints que são alvo destes pedidos, que não estão registados sobre nenhum domínio. Alguns endereços que estão registados sobre um domínio, dão sinal de maliciosos, como o caso de “zy.3gogo.net.cn” e “ls.3gogo.net.cn”. É ainda apresentada a informação de que a aplicação contém um ou mais ficheiros executados pelo sistema operativo Linux.