Decode xHelper - the kind of immortal malicious code on Android, still 'alive' after factory reset

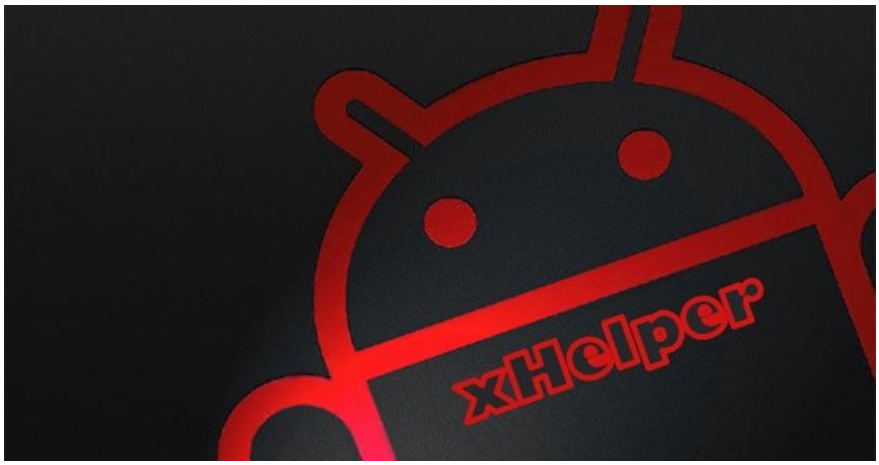
Recently, researchers at Kaspersky Labs have discovered the extremely complex operation of xHelper, a new malware that attacks devices running Android, capable of surviving even after performing a factory reset. Return to original settings.

Recently, researchers at Kaspersky Labs have discovered the extremely complex operation of xHelper, a new malware that attacks devices running Android, capable of surviving even after performing a factory reset. Return to original settings.

Basically, xHelper or its variants will install itself into the system partition of Android phone after gaining root privileges. Even malicious code can force the system to change to remove this malware from the phone more difficult.

The problem is that the system partition usually doesn't allow overwriting. Normally, the system partition only grants 'read-only' permission to users, so removing applications that contain malware is not a problem. More troublesome, this malware is also given the data files that it has written to the system partition for greater permissions, even the root of the machine is not easy to solve.

The creators of xHelper also provide this malicious code with an extremely bizarre feature that allows changing the libc system library of the Android operating system itself, disabling the conversion of the system partition from read-only to write. mode, even automatically uninstall root apps.



To remove xHelper, users will have to recover the device, either flash the device with the original installation or replace the system component in the device.

However, this malware downloaded a rootkit to hijack the machine. And this rootkit mainly infects older versions of Android like 6 and 7, on some kind of Chinese 'fake smartphones'. Security researchers have discovered malware in the original phone carrier so they don't have to live with xHelper users to find a more reputable ROM or buy a new phone!