Trojan infection when using KakaoTalk

Trend Micro, a security firm in Japan, recently discovered KakaoTalk and many other messaging applications are becoming targets of hackers 'attacks, threatening users' information security.

Trend Micro, a security firm in Japan, recently discovered KakaoTalk and many other messaging applications are becoming targets of hackers 'attacks, threatening users' information security.

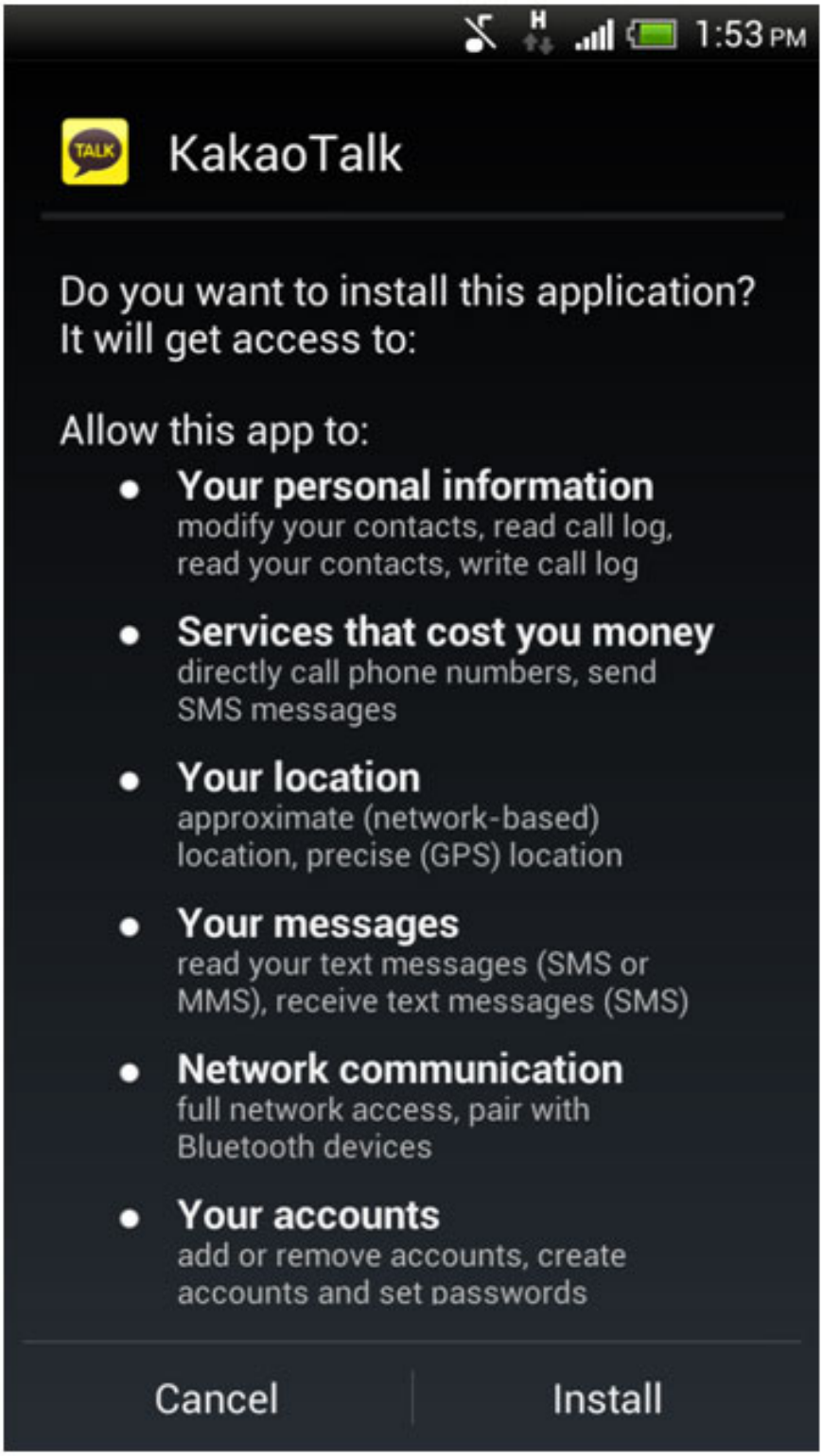
One of the most sophisticated ways for hackers to attack users is to write a legitimate version of popular applications and add malicious code to it. This will create an application containing trojans, but users will not know what is the real version and what is the malicious version.

In the case of the recent discovery in Japan, the malicious trojan version of KakaoTalk was discovered named **ANDROIDOS_ANALITYFTP.A.** This version has been spread through email. If you compare detailed applications, users can see the differences between versions.

	Legitimate: com.kakao.talkJ	Repackaged app: com.kakao.talk
Version	3.5.5	3.5.5
Organization Unit	kakaoteam	asd
Organization	kakao	zxc
Location		rty
State		fgh
Country	ko	vbn
Serial Number	4c707197	a3e5475
Valid	from: Sun Aug 22 08:38:47 CST 2010 to: Tue Jul 29 08:38:47 CST 2110	from: Wed Jan 09 11:45:49 CST 2013 to: Thu Oct 13 11:45:49 CST 2067

Differences between legal (left) and malicious KakaoTalk versions (right).

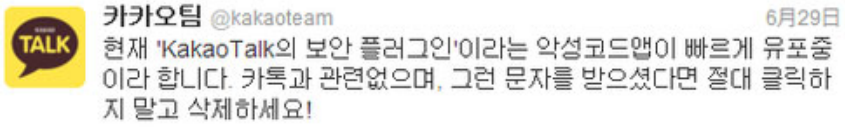
In addition, users also have a way to distinguish between the original application version and the trojan version. It is trojan applications that always require **more access** than legitimate applications.



The Trojan version always requires more permissions.

ANDROIDOS_ANALITYFTP.A is identified as a trojan of tracking nature. Taking advantage of the invariant in the Android programming language, Java, the attacker will set up applications that regularly send owners contact information, text messages . This data can become a platform. for the next attack.

Besides creating malicious trojan application versions, the fake application is also used in KakaoTalk case. About a month ago, KakaoTalk warned users, through their official Twitter account, about a **"KakaoTalk Security Plugin".**



KakaoTalk notifications from Twitter.

This fake application is known as **ANDROIDOS_FAKEKKAO.A.** A lot of people have been tricked for being named KakaoTalk, and then **"Security"** feels safe for users to download.

Fake software is inserted into legitimate software.

Prevention:

The best way to prevent these threats is to **avoid downloading** applications outside of Google Play. Even, users should check the legality of current applications, to detect trojan versions. In addition, using a security solution like **Trend Micro Mobile Security** for mobile devices is also a must.

Besides the wise use of users, the responsibility of the application developers should also be emphasized. When creating and deciding to market, developers need to evaluate software, this application is at risk of being exploited, installing trojans or not. This not only helps users, but will also affect the reputation of the application developer itself.