Source code for powerful Android banking malware is leaked

pcworld.com/article/3035725/source-code-for-powerful-android-banking-malware-is-leaked.html

By Jeremy Kirk

The source code for a powerful Android malware program that steals online banking credentials has been leaked, according to researchers with IBM.

The malware family is known by several names, including GM Bot, Slempo, Bankosy, Acecard, Slempo and MazarBot.

GM Bot has been sold on underground hacking forums for around US$500. But it appears someone who bought the code then leaked it on a forum in December, perhaps to increase his standing, wrote Limor Kessem, a cybersecurity analyst with IBM Trusteer.

The person included an encrypted archive file containing the source code of GM Bot, according to Kessem.

“He indicated he would give the password to the archive only to active forum members who approached him,” Kessem wrote. “Those who received the password in turn passed it on to other, unintended users, so the actual distribution of the code went well beyond that discussion board’s member list.”

The source code of powerful banking trojans has been leaked before with apps such as Zeus, SpyEye and Carberp, Kessem wrote.

“While GM Bot may not be as prolific as the major banking Trojans mentioned here, it is definitely a game changer in the realm of mobile threats,” Kessem added.

GM Bot emerged in late 2014 on Russian-speaking forums. It exploits an issue known as activity hijacking in older Android devices that allow an overlay to be displayed over a legitimate application.

Google has put in defenses against activity hijacking in Android versions higher than 5.0.

The overlay looks like what a user would expect to see after launching a legitimate banking app, but that app is actually running underneath the overlay. The user then inputs their authentication credentials, which are sent to the attackers.

Since GM Bot has full control over the device, it can also steal SMSes, such as one-time authentication codes.

“Previous mobile malware — before overlays became commercially available to fraudsters — could steal SMS codes, but those would have been meaningless without phishing schemes or a trojan on the victim’s PC to steal access credentials,” Kessem wrote.

Since the leak of GM Bot’s code, it appears its creators have developed a second version “which is sold in financial fraud-themed underground boards,” Kessem wrote.

Note: When you purchase something after clicking links in our articles, we may earn a small commission. Read our affiliate link policy for more details.

Related:

- Security