EXHIBIT 4

DroidDream Light a malware nightmare, booted from Android Market

By Ryan Paul | Published 6 days ago

A number of malware-encumbered applications were found in the Android Market back in March, but the infestation was brought to a swift end when Google deployed its kill switch. A new variant of the same malware recently resurfaced and was identified by security researchers over the weekend. Google has responded by booting the new round of infected applications out of the Android Market.

The malware was discovered by Lookout, a mobile security company. They found just under 30 infected applications across six separate developer accounts. Several of the infected applications were existing third-party programs that the attacker copied and then repackaged with the malware.

The malware-bearing programs spanned a diverse range of functions, including a scientific calculator, a solitaire game, and a photo enhancement tool. Malicious developer Magic Photo Studio had the most colorful assortment of infected apps, including a soundboard called Sex Sound and a photo gallery program called Beauty Breasts.

The infected applications appear to have been widely downloaded prior to being shut down by Google. Lookout estimates that between 30,000 and 120,000 users have been affected by the attack. We used Google Cache to examine the Android Market pages for several of the malicious apps. The Beauty Breasts program had a 3.5 star rating and been installed between 1,000 and 5,000 times.

The new malware is based on the same code that was used back in March, but it is simpler and has some limitations that make it less potentially dangerous. The original March flavor would attempt to root the victim's phone so that it could install additional software without requiring intervention by the user. The new variant still has the capability to download and install additional software, but it doesn't take root access and consequently has to prompt the user before it can install anything.

Lookout is calling the variant DroidDream Light. Like the previous version, Droid Dream Light will send information back to a command-and-control server. The malware can apparently do its dirty work even if the user never actually runs the application. It hooks into the platform's event system APIs and will launch itself as a background process when the device's call state changes—like when a call is received.

It's worth noting that hooking into the phone's state requires a special permission that is listed when the user installs the application from the Android Market. A savvy user who is paying attention to the permissions would likely realize that phone state monitoring isn't needed for looking at images of breasts and would hopefully think twice before installing the program.

This latest round of Android malware makes it seem like the problem isn't going to go away. Although Google responded to the threat very quickly after it was detected, the number of users who downloaded the applications is still troubling. Armed with a remote kill switch and full control over the Android Market, Google can address threats as they arise, but can't really provide a proactive safety net.

Further reading

- Lookout (blog.mylookout.com)