



## Infected Android app runs up big texting bills

Hackers up ante by adding more malicious 'features' to legitimate smartphone apps, says Symantec

Gregg Keizer

February 28, 2011 ([Computerworld](#))

A rogue Android app that's been tweaked by hackers can hijack a smartphone and run up big texting bills before the owner knows it, Symantec said today.

The newest in a line of compromised Android apps, said Vikram Thakur, a principle security response manager at Symantec, is [Steamy Window](#), a free program that Chinese hackers have modified, then re-released into the wild.

The cyber criminals grabbed a copy of Steamy Windows, then added a backdoor Trojan horse - "Android.Pjapps" by Symantec's label -- to the app's code. The reworked app is then placed on unsanctioned third-party "app stores" where unsuspecting or careless Android smartphones find it, download it and install it.

"This one stands out," said Thakur on Monday. "It's pretty comprehensive in what it's doing."

The Trojan planted by the malware-infected Steamy Windows can install other applications, monkey with the phone's browser bookmarks, surreptitiously navigate to Web sites and silently send text messages, said Thakur.

The last is how the criminals make money.

"The Trojan lets them send SMS [short message service] messages to premium rate numbers," said Thakur, for which the hackers are paid commissions.

Android.Pjapps also has a built-in filter that blocks incoming texts from the user's carrier, a trick it uses to keep victims in the dark about the invisible texting.

"It monitors inbound SMS texts, and blocks alerts telling you that you've already exceeded your quota," Thakur said. Smartphone owners then wouldn't be aware of the charges they've racked up texting premium services until they receive their next statement.

Symantec found the cloned Steamy Windows app on a Web site hosted by Chinese servers.

The practice of altering legitimate Android apps to carry malware isn't new -- earlier this year, security experts warned that [Monkey Jump was being cloned](#) by criminals for the same purpose -- but the bogus Steamy Window app shows that hackers are getting better at reworking mobile software.

"The code inside [Steamy Windows] can be easily added to other apps," said Thakur today. "For someone who knows what they're doing -- and it seems these people have a good understanding of how apps are coded -- I'd put this in the 'trivial to do' category. The last few months, it seems to be ramping up."

Android smartphones are an attractive target for hackers, Thakur continued, because of their increasing popularity and because, unlike Apple's iOS, users can install apps downloaded from third-party distribution sites.

"Where there's honey, there's bees," said Thakur.


Smartphone owners should be wary of unauthorized app stores, Thakur said. "Downloading an app from one of these [third-party] sites is like downloading a Windows app from a 'warez' site," he

said, referring to sites that post illegally-obtained content, which often is malware infected.

"And if you're hell-bent on using them, look at the permissions the app requests when it installs. A [rogue] app will request more permissions than the legitimate version," he said.

Symantec published an [analysis of Android.Pjapps](#) on its Web site Monday.

The [legitimate Steamy Window app](#) for Android can be downloaded from Google's Android Market.

**Gregg Keizer** covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at [@gkeizer](#), or subscribe to [Gregg's RSS feed](#) . His e-mail address is [gkeizer@ix.netcom.com](mailto:gkeizer@ix.netcom.com).