Virulent Android malware returns, gets >2 million downloads on Google Play

By Dan Goodin

Published: 2017-01-23 · Archived: 2026-04-06 00:06:16 UTC

A virulent family of malware that infected more than 10 million Android devices last year has made a comeback, this time hiding inside Google Play apps that have been downloaded by as many as 12 million unsuspecting users.

HummingWhale, as the professionally developed malware has been dubbed, is a variant of HummingBad, the name given to a family of malicious apps researchers documented in July invading non-Google app markets. HummingBad attempted to override security protections by exploiting unpatched vulnerabilities that gave the malware root privileges in older versions of Android. Before Google shut it down, it installed more than 50,000 fraudulent apps each day, displayed 20 million malicious advertisements, and generated more than $300,000 per month in revenue. Of the 10 million people who downloaded HummingBad-contaminated apps, an estimated 286,000 of them were located in the US.

HummingWhale, by contrast, managed to sneak its way into about 20 Google Play apps that were downloaded from 2 million to 12 million times, according to researchers from Check Point, the security company that has been closely following the malware family for almost a year. Rather than rooting devices, the latest variant includes new virtual machine techniques that allow the malware to perform ad fraud better than ever, company researchers said in a blog post published Monday.

“Users must realize that they can no longer trust in installing only apps with a high reputation from official app stores as their sole defense,” the researchers wrote in an e-mail to Ars. “This malware employs several tactics to keep its activity hidden, meaning users might be unaware of its existence on their device.”

As was the case with HummingBad, the purpose of HummingWhale is to generate revenue by displaying fraudulent ads and automatically installing apps. When users try to close the ads, the new functionality causes already downloaded apps to run in a virtual machine. That creates a fake ID that allows the perpetrators to generate referral revenues. Use of the virtual machine brings many technical benefits to the operators, chief among them allowing the malware to install apps without requiring users to approve a list of elevated permissions.
