Masterhacks – La empresa Kaspersky Lab alertó sobre el descubrimiento de un nuevo tipo de malware que se ha distribuido entre los usuarios de Android, por medio de la Play Store.

El malware es un troyano al que denominaron Dvmap, mismo que logró burlar la seguridad de Google en su tienda de aplicaciones.

“Para eludir los controles de seguridad de la tienda, los creadores subieron una app libre de malware a la tienda a finales de marzo de 2017. Posteriormente la actualizaron con una versión maliciosa por un corto período de tiempo, antes de volver a subir otra versión libre de malware. En un periodo de cuatro semanas hicieron esto al menos cinco veces”, afirman los investigadores de Kaspersky.

Asimismo, la empresa estima que el troyano se ha descargado más de 50 mil veces desde que apareció en marzo.

Cuanto este malware se instala en el dispositivo, inyecta un código malicioso en las bibliotecas del sistema y elimina los derechos de root.

Una vez hecho esto, los atacantes pueden enviar comandos por medio de un servidor para descargar e instalar más apps maliciosas, sin embargo, Kaspersky afirma que no se han observado comandos enviados, por lo que es posible que los piratas sólo hayan estado verificando la efectividad del malware antes de un ataque masivo.

“Todo indica que el objetivo principal de Dvmap es entrar en el sistema y ejecutar los archivos descargados con derechos de root. Pero yo nunca recibí este tipo de archivos de sus servidores de comando y control”, dijo Roman Unuchek, analista de Kaspersky Lab.

Según Unuchek, el malware se distribuyó por medio de la app Colourblock, y recomienda que en caso de haber sido infectado y no contar con un antivirus, se respalde la información del dispositivo y restablecer las configuraciones de fábrica.