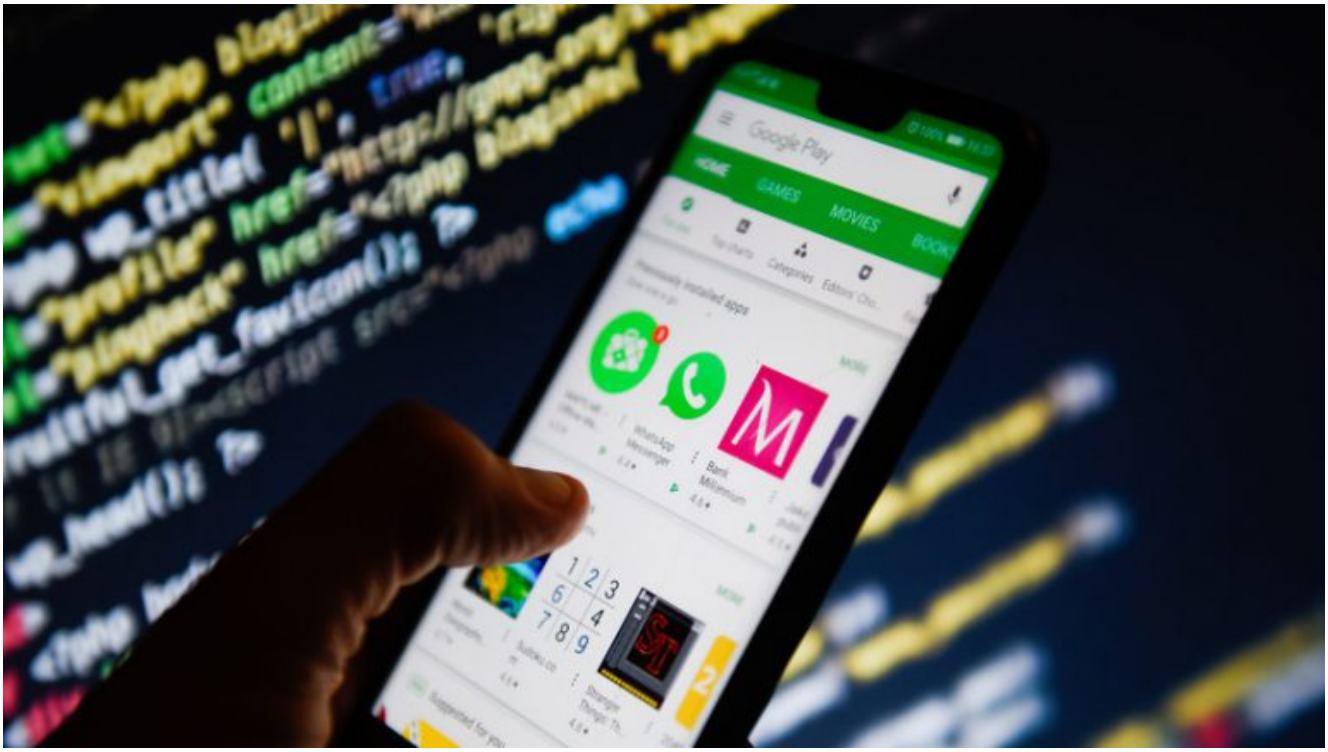

Detectan el nuevo virus ‘Joker’, descargado ya casi 500.000 veces y que roba dinero a sus víctimas

El analista de ‘malware’ de la empresa CSIS Security Group, Aleksejs Kuprins, ha detectado un nuevo troyano llamado ‘Joker’ en 24 aplicaciones de Google Play, el cual no solo puede robar los datos personales de los usuarios, sino también su dinero en tiempo real, de acuerdo con un artículo, publicado el pasado martes en el portal Medium.

El virus, que obtuvo su nombre de uno de los servidores de control y comando (C&C) descubierto por los investigadores de CSIS, está destinado para inscribir silenciosamente a los usuarios en los servicios de suscripción premium y de esta

manera robarles hasta 7 dólares por semana, como fue detectado por Kuprins en el caso de Dinamarca.

¿Cómo funciona el virus?

En detalle, 'Joker' **simula el proceso que un usuario realizaría para registrarse**. Así, el componente de fondo de estas aplicaciones, que en total fueron descargadas más de 472.000 veces, silenciosamente hace un clic en un anuncio dentro de la 'app' y luego hace lo mismo para el proceso de inscripción cuando ya está en el sitio web. Luego, el virus **accede a los mensajes SMS** de la víctima, copiando el código de autorización que fue enviado para verificar los pagos de suscripción.

El experto subrayó que es difícil notar la existencia de estas suscripciones a menos que un usuario sea muy diligente en verificar su estado de cuenta mensual de la tarjeta de crédito. Además, se informa que 'Joker' puede **robar la lista de contactos** de la víctima y la información sobre su dispositivo.

De acuerdo con Kuprins, **37 países**, incluidos EE.UU., Argentina, Brasil y España, pueden estar afectados por el virus. Sin embargo, el analista subrayó que algunas de las citadas aplicaciones no tienen restricciones regionales.

No obstante, se informa que Google ya eliminó las 24 aplicaciones de su tienda, pero Kuprins aconseja revisar el historial de transacciones, así como siempre prestar mucha atención a la lista de permisos a los que tiene acceso una u

otra ‘app’.

Fuente: **RT Actualidad**