Un nuevo malware para Android llamado RatMilad se ha observado dirigido a dispositivos móviles empresariales de Oriente Medio al ocultarse como una VPN y una aplicación de suplantación de números de teléfono.

El troyano móvil funciona como software espía avanzado con capacidades de recibir y ejecutar comandos para recopilar y filtrar una amplia variedad de datos del terminal móvil infectado, según informó Zimperium.

La evidencia recopilada por la compañía de seguridad móvil muestra que la aplicación maliciosa se distribuye por medio de enlaces en las redes sociales y herramientas de comunicación como Telegram, engañando a los usuarios desprevenidos para que descarguen la aplicación y les otorguen amplios permisos.

La idea detrás de la incrustación del malware dentro de una VPN falsa y un servicio de suplantación de números de teléfono resulta algo inteligente, ya que la aplicación afirma permitir a los usuarios verificar las cuentas de las redes sociales a través del teléfono, una técnica popular en países donde el acceso está restringido.

> *«Una vez instalado y en control, los atacantes pueden acceder a la cámara para tomar fotos, grabar audio y video, obtener ubicaciones GPS precisas, ver imágenes desde el dispositivo y más»,* dijo Nipun Gupta, investigador de Zimperium.

Otras características de RatMilad hacen posible que el malware acumule información de la SIM, datos del portapapeles, mensajes SMS, registros de llamadas, listas de contactos e incluso realice operaciones de lectura y escritura de archivos.

Zimperium planteó la hipótesis de que los operadores responsables de RatMilad adquirieron el código fuente de un grupo de hackers iraníes denominado AppMilad, y lo integraron en una aplicación fraudulenta para distribuirla a usuarios involuntarios.

Se desconoce la escala de las infecciones, pero la compañía de seguridad cibernética dijo

que detectó el software espía durante un intento fallido de compromiso del dispositivo empresarial de un cliente.

Una publicación compartida en un canal de Telegram utilizado para propagar la muestra de malware, se ha visto más de 4700 veces con más de 200 recursos compartidos externos, lo que indica un alcance limitado.

> *«El software espía RatMilad y el grupo de hackers con sede en Irán, AppMilad, representan un entorno cambiante que afecta la seguridad de los dispositivos móviles»,* dijo Richard Melick, director de inteligencia de amenazas móviles de Zimperium.

> *«Desde Pegasus hasta PhoneSpy, existe un creciente mercado de spyware móvil disponible por medio de fuentes legítimas e ilegítimas, y RatMilad es solo uno de ellos»*.