Noticia: Piratas informáticos palestinos que difunden software espía móvil

- **¿Qué tipo de amenaza es?**

La amenaza es de tipo spyware.

- **¿Cómo comienza y cómo se propaga esta amenaza?**

Se aprovechó la plataforma de Facebook como un trampolín para lanzar una variedad de ataques de ingeniería social en un intento de atraer a la gente a hacer clic en enlaces maliciosos e instalar malware en sus dispositivos.

Se usó un malware de Android personalizado que se disfrazó como aplicaciones de chat seguras para capturar de manera sigilosa metadatos del dispositivo, capturar pulsaciones de teclas y cargar los datos en Firebase

Facebook sospecha que Arid Viper utilizó el malware iOS sólo en un puñado de casos, sugiriendo una operación altamente dirigida, con los hackers vinculados a Hamas simultáneamente centrándose en un conjunto en evolución de aplicaciones de spyware basadas en Android que afirmaban facilitar las citas, las redes y la banca regional en el Medio Oriente, con el adversario enmascarando el malware como actualizaciones de aplicaciones falsas para aplicaciones legítimas como WhatsApp.

Una vez instalado, el malware instó a las víctimas a desactivar Google Play Protect y dar permisos de administrador del dispositivo de la aplicación, utilizando el acceso arraigado a las llamadas de grabación, capturar fotos, audio, vídeo o capturas de pantalla, interceptar mensajes, rastrear la ubicación del dispositivo, recuperar contactos, registros de llamadas y detalles del calendario, e incluso información de notificación de aplicaciones de mensajería como WhatsApp, Instagram, Imo, Viber y Skype.

- **¿Hay más de una amenaza aplicada ?**

  Troyanos, gusanos y spyware

https://thehackernews.com/2021/04/facebook-busts-palestinian-hackers.html