Centro Nacional de Seguridad Digital	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°279**	**Fecha: 22-11-2023**
		Página: 4 de 10

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Los ciberdelincuentes se dirigen a los usuarios indios con campañas engañosas de troyanos de banca móvil a través de WhatsApp y Telegram		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. **ANTECEDENTES:**

Un aumento alarmante en las campañas de troyanos bancarios móviles ha puesto en riesgo a los usuarios indios, y los ciberdelincuentes aprovechan plataformas de redes sociales populares como WhatsApp y Telegram para lanzar esquemas engañosos. Estas campañas tienen como objetivo engañar a usuarios desprevenidos para que instalen aplicaciones maliciosas haciéndose pasar por servicios legítimos ofrecidos por bancos y entidades gubernamentales.

Estas campañas malévolas, según revelan investigadores de Microsoft , han adoptado tácticas más sofisticadas para infiltrarse en los dispositivos de los usuarios. A diferencia de los métodos anteriores que se basaban en enlaces maliciosos, las estrategias más recientes implican compartir directamente archivos APK fraudulentos, imitando aplicaciones bancarias conocidas, para explotar la confianza que los usuarios depositan en estas instituciones.

2. **DETALLES:**

La investigación inicial reveló el modus operandi de estas campañas. En un caso, los ciberdelincuentes iniciaron una campaña de phishing en WhatsApp, distribuyendo un mensaje engañoso que contenía un archivo APK malicioso que se hacía pasar por una aplicación bancaria oficial. El mensaje afirmaba falsamente que la cuenta bancaria del usuario enfrentaba un bloqueo inminente, obligándolo a actualizar su tarjeta PAN (número de cuenta permanente) a través del enlace proporcionado.

Tras la instalación, la aplicación engañosa recopiló sigilosamente datos confidenciales, incluida información personal, credenciales bancarias y detalles de tarjetas de pago. La interfaz de la aplicación imitaba fielmente la de las aplicaciones bancarias legítimas, engañando a las víctimas para que revelaran sus números de móvil, pines de cajero automático y detalles de la tarjeta PAN. Posteriormente, las víctimas fueron obligadas a creer que eliminar la aplicación interrumpiría el proceso de verificación en curso, manteniendo la aplicación fraudulenta ejecutándose en segundo plano y ocultando sus actividades maliciosas al usuario.

En otro caso, una táctica paralela se centró en los datos de las tarjetas de pago de los usuarios, amplificando el riesgo de fraude financiero. La aplicación maliciosa, aunque solicitaba datos personales como nombres, ID de correo electrónico, números de teléfono móvil y fechas de nacimiento, tenía como objetivo particular robar datos específicos de tarjetas de crédito, lo que representa una grave amenaza para la seguridad financiera de los usuarios.

3. **RECOMENDACIONES:**

- Descargar e instalar aplicaciones únicamente de tiendas autorizadas o de los sitios web oficiales de sus respectivos bancos.
- Desactivar la función "Instalar aplicaciones desconocidas" en dispositivos Android para mitigar riesgos potenciales.
- Aplicar prácticas de seguridad estrictas para protegerse contra posibles amenazas cibernéticas.
- Capacitar a los usuarios sobre las mejores prácticas de ciberseguridad.

Fuente de Información:	• hxxps://www.the420.in/indian-users-threatened-mobile-trojan-campaigns-micosoft/