Después de 4 meses de haber descubierto «Tetrade«, un conjunto de cuatro troyanos bancarios brasileños dirigidos a instituciones financieras en Brasil, América Latina y Europa, nuevos hallazgos demuestran que los delincuentes detrás de la operación han ampliado sus tácticas para infectar dispositivos móviles con software espía.

Según el equipo de análisis e investigación global de Kaspersky (GReAT), el grupo de amenazas con sede en Brasil, Guildma, implementó Ghimob, un troyano bancario de Android dirigido a aplicaciones financieras de bancos, empresas de tecnología, intercambios y criptomonedas en Brasil, Paraguay, Perú, Portugal, Alemania, Angola y Mozambique.

> *«Ghimob es un espía de pleno derecho en su bolsillo: una vez que se completa la infección, el pirata informático puede acceder al dispositivo infectado de forma remota, completando la transacción fraudulenta con el teléfono inteligente de la víctima, para evitar la identificación de la máquina, las medidas de seguridad implementadas por las instituciones financieras y todos sus sistemas de comportamiento antifraude»*, dijo la compañía de seguridad.

Además de compartir la misma infraestructura que Guildma, Ghimob sigue el modus operandi de utilizar correos electrónicos de phishing como un mecanismo para distribuir el malware, atrayendo así a los usuarios desprevenidos a hacer clic en URL maliciosas que descargan el instalador APK de Ghimob.

Una vez instalado el troyano, funciona de forma similar a otros RAT móviles en el sentido de que enmascara su presencia ocultando el icono del cajón de la aplicación y abusa de las funciones de accesibilidad de Android para ganar persistencia, deshabilitar la desinstalación manual y permitir que el troyano bancario capture pulsaciones de teclas, manipule el contenido de la pantalla y proporcione un control remoto completo al atacante.

> *«Incluso si el usuario tiene un patrón de bloqueo de pantalla, Ghimob puede grabarlo y luego reproducirlo para desbloquear el dispositivo»,* dijeron los

> investigadores.
>
> *«Cuando el ciberdelincuente está listo para realizar la transacción, puede insertar una pantalla negra como una superposición o abrir algún sitio web en pantalla completa de modo que mientras el usuario mira esa pantalla, el delincuente realiza la transacción en segundo plano utilizando la aplicación financiera ejecutándose en el teléfono inteligente de la víctima que el usuario ha abierto o en el que ha iniciado sesión»,* agregaron.

Ghimob apunta a 153 aplicaciones móviles, 112 de las cuales son instituciones financieras con sede en Brasil, y las aplicaciones bancarias y de criptomonedas en Alemania, Portugal, Perú, Paraguay, Angola y Mozambique representan el resto.

> *«Ghimob es el primer troyano bancario móvil brasileño listo para expandirse y apuntar a instituciones financieras y sus clientes que viven en otros países. El troyano está bien preparado para robar credenciales de bancos, fintechs, intercambios, intercambios de cifrado y tarjetas de crédito de instituciones financieras que operan en muchos países»,* concluyó Kaspersky.