Se ha identificado una nueva vulnerabilidad en Android con habilidades significativas para ejecutar diversas acciones dañinas en los dispositivos comprometidos.

Llamado Xamalicious por el Equipo de Investigación Móvil de McAfee, este software malicioso toma su nombre del uso de un marco de desarrollo de aplicaciones móviles de código abierto llamado Xamarin, aprovechando los permisos de accesibilidad del sistema operativo para alcanzar sus metas.

Además, tiene la capacidad de recolectar información técnica sobre el dispositivo afectado y establecer comunicación con un servidor central de control (C2) para descargar una carga adicional, siempre que sea adecuada para su propósito.

Una vez descargada, esta carga *«se integra dinámicamente como un archivo DLL en el momento de ejecución, permitiéndole obtener control absoluto del dispositivo y posiblemente realizar operaciones engañosas, como generar clics en publicidades, descargar aplicaciones no deseadas, entre otras actividades fraudulentas sin el conocimiento del usuario»,* mencionó Fernando Ruiz, experto en seguridad.

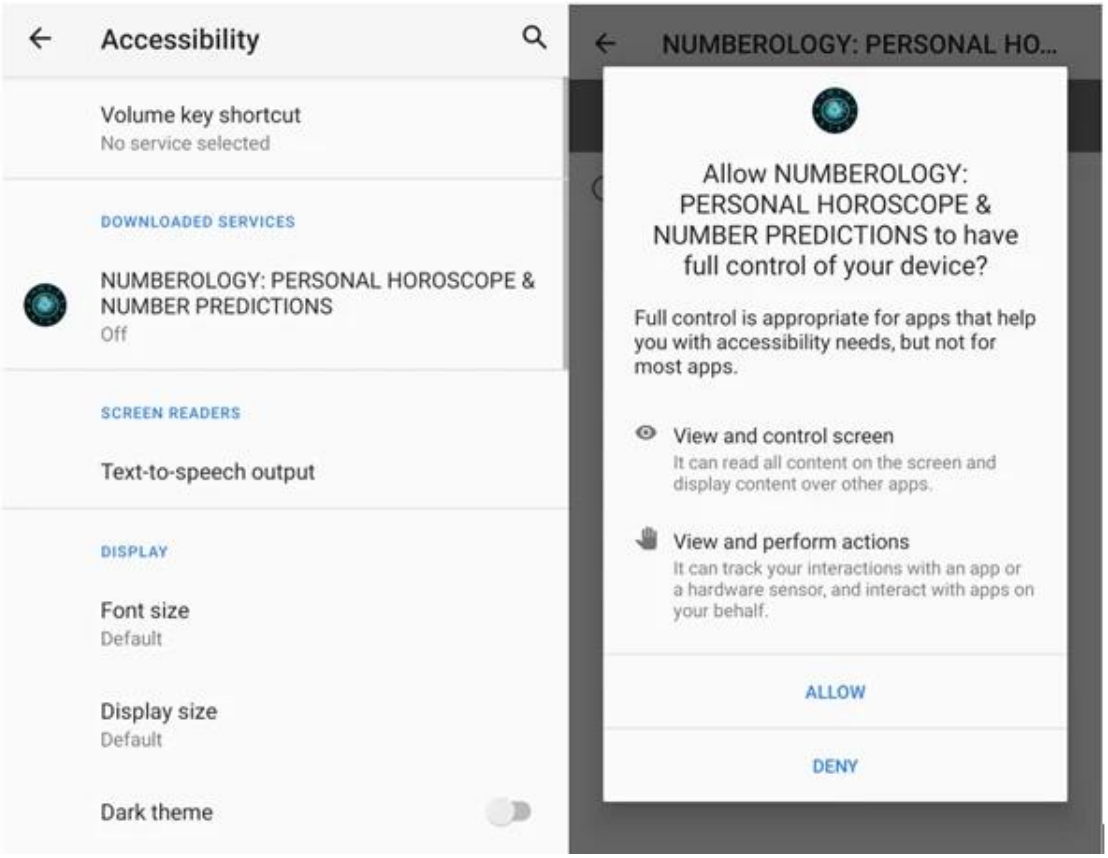
La compañía especializada en seguridad digital informó que detectaron 25 aplicaciones que incluyen este software dañino. Algunas de estas aplicaciones han estado disponibles en la tienda oficial de Google Play desde el 2020. Se calcula que se han descargado al menos en 327,000 ocasiones.

Las regiones más afectadas han sido Brasil, Argentina, Reino Unido, Australia, Estados Unidos, México y varios países de Europa y América. A continuación, se detallan algunas de las aplicaciones mencionadas:

- Horóscopo Esencial para Android (com.anomenforyou.essentialhoroscope)
- Editor 3D de Pieles para Minecraft PE (com.littleray.skineditorforpeminecraft)
- Creador de Logotipos Pro (com.vyblystudio.dotslinkpuzzles)
- Repetidor Automático de Clics (com.autoclickrepeater.free)
- Calculadora Simplificada de Calorías (com.lakhinstudio.counteasycaloriecalculator)

- Amplificador de Sonido para Dispositivos (com.muranogames.easyworkoutsathome)
- Conecta Letras (com.regaliusgames.llinkgame)
- NUMEROLOGÍA: Horóscopo Personal y Pronósticos de Números (com.Ushak.NPHOROSCOPENUMBER)
- Monitor de Pasos: Contador de Pasos Fácil (com.browgames.stepkeepereasymeter)
- Registro de Tu Sueño (com.shvetsStudio.trackYourSleep)
- Potenciador de Volumen de Sonido (com.devapps.soundvolumebooster)
- Guía Astrológica: Horóscopo Diario y Lecturas del Tarot (com.Osinko.HoroscopeTaro)
- Calculadora para Todo (com.Potap64.universalcalculator)

Xamalicious, que a menudo se presenta como aplicaciones relacionadas con salud, juegos, astrología y herramientas de productividad, se suma a una lista creciente de programas maliciosos que explotan los servicios de accesibilidad en dispositivos Android, solicitando permisos al usuario durante la instalación para sus propios fines.

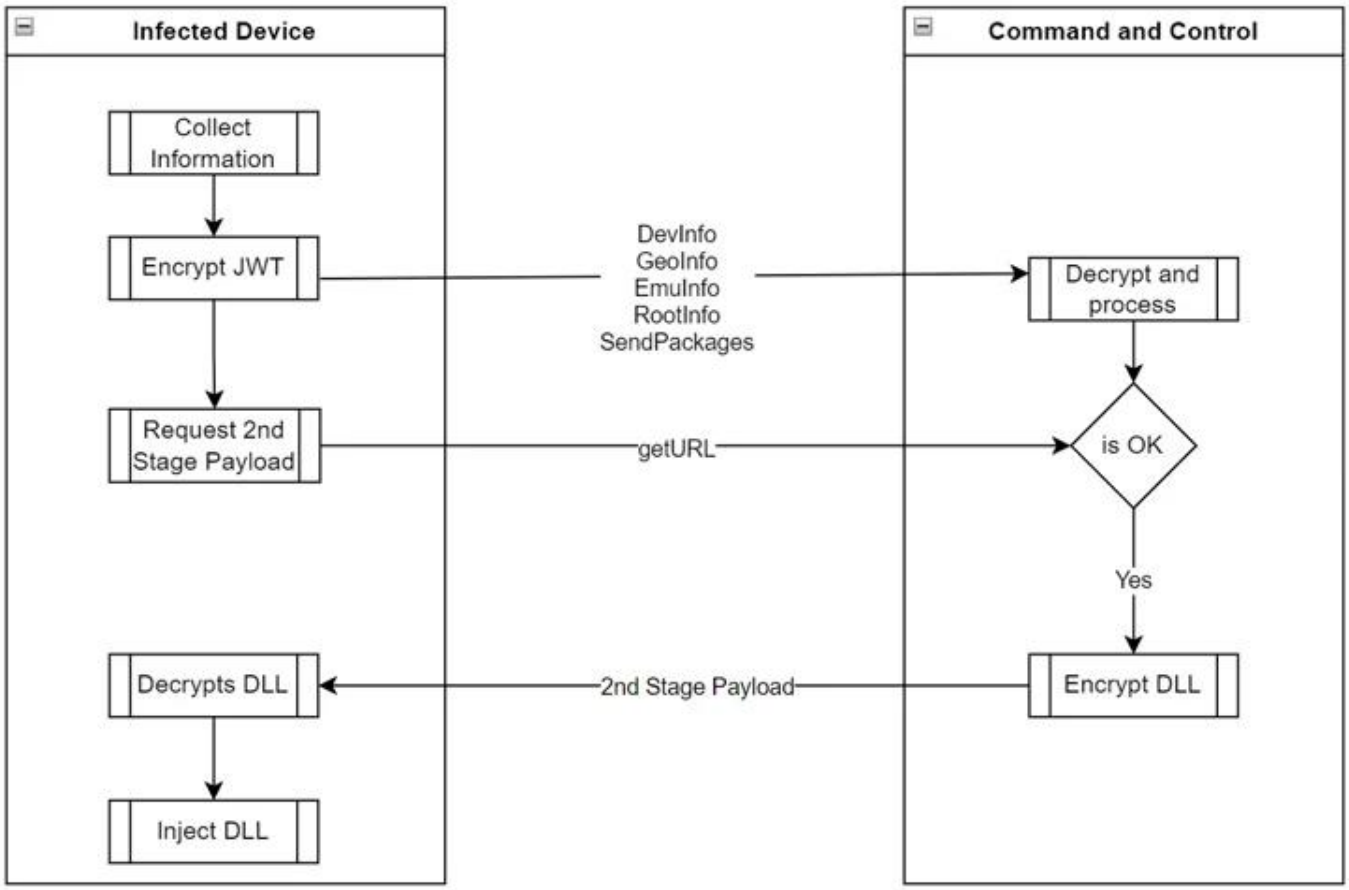


> *«Para burlar las medidas de análisis y detección, los creadores de malware han encriptado todas las comunicaciones y datos entre el C2 y el dispositivo comprometido. No se trata solo de una protección con HTTPS, sino que se emplea un token de Encriptación Web JSON (JWE) con el método RSA-OAEP utilizando el algoritmo 128CBC-HS256,»* explicó Ruiz.

Más preocupante aún, el archivo inicial de este malware tiene capacidades para actualizar automáticamente el archivo principal (APK) de Android. Esto implica que puede ser utilizado de manera maliciosa, ya sea como herramienta de espionaje o como troyano bancario, sin necesidad de interacción por parte del usuario.

McAfee informó que detectó una relación entre Xamalicious y una aplicación fraudulenta de publicidad llamada Cash Magnet. Esta aplicación facilita descargas y activa clics automáticos para generar ingresos fraudulentos mediante publicidad.

> *«Las aplicaciones de Android desarrolladas con tecnologías como Flutter, react native y Xamarin ofrecen un nivel adicional de confusión para aquellos que crean malware. Estos creadores de malware escogen estas plataformas específicamente para pasar desapercibidos y evitar la detección de expertos en seguridad, manteniendo así su presencia en tiendas de aplicaciones,»* agregó Ruiz.



Campaña de Phishing en Android enfocada en India con Malware Bancario

Estos hallazgos emergen cuando una firma de ciberseguridad destaca una campaña de phishing que utiliza aplicaciones de mensajería como WhatsApp. Estas aplicaciones distribuyen archivos APK engañosos que simulan ser de bancos legítimos, como el Banco Estatal de la India (SBI), instando a los usuarios a instalarlos bajo el pretexto de un proceso KYC obligatorio.

Una vez dentro del dispositivo, la aplicación solicita permisos relacionados con SMS y luego lleva al usuario a un sitio web falso. Este sitio no solo roba las credenciales de acceso del usuario sino también datos sensibles como números de cuenta y detalles de tarjetas.

Los datos recolectados, junto con mensajes SMS interceptados, se envían a servidores controlados por los atacantes, permitiéndoles realizar transacciones sin autorización.

Es importante mencionar que, recientemente, Microsoft advirtió sobre tácticas similares utilizando plataformas como WhatsApp y Telegram, dirigidas específicamente a usuarios bancarios de la India.

> *«El panorama digital de la India muestra una vulnerabilidad significativa ante este tipo de malware bancario, con incidentes detectados también en otras regiones, posiblemente relacionados con usuarios del SBI en el extranjero,»* comentaron los expertos Neil Tyagi y Ruiz.