Los expertos en ciberseguridad han expuesto una compleja campaña de phishing móvil (también conocida como mishing) diseñada para propagar una versión actualizada del troyano bancario Antidot.

> *«Los ciberdelincuentes se hacían pasar por reclutadores, atrayendo a víctimas desprevenidas con ofertas laborales tentadoras»*, señaló Vishnu Pratapagiri, investigador de Zimperium zLabs, en un informe reciente.
>
> *«Como parte de este falso proceso de contratación, la campaña engaña a las víctimas para que instalen una aplicación maliciosa que funciona como dropper, lo que finalmente lleva a la instalación de una nueva variante del Antidot Banker en el dispositivo afectado».*

Esta nueva versión del malware para Android ha sido bautizada como AppLite Banker por la empresa de seguridad móvil, destacando su capacidad para capturar PIN de desbloqueo, patrones o contraseñas, así como para tomar control remoto de los dispositivos infectados. Una funcionalidad similar ha sido vista en TrickMo recientemente.

El ataque utiliza diversas tácticas de ingeniería social, generalmente ofreciendo trabajos con atractivas condiciones, como un *«salario competitivo de $25 por hora»* y prometedoras opciones de desarrollo profesional.

En septiembre de 2024, Se encontró en Reddit publicaciones de usuarios que afirmaban haber recibido correos electrónicos de una empresa canadiense llamada Teximus Technologies ofreciendo empleos remotos como agentes de atención al cliente.

Si las víctimas aceptaban interactuar con el supuesto reclutador, eran redirigidas a descargar una aplicación maliciosa de Android desde una página de phishing, presentada como parte del proceso de contratación. Esta aplicación actuaba como la primera etapa para introducir el malware principal en los dispositivos de los usuarios.

Zimperium informó haber descubierto una red de dominios falsos usados para distribuir archivos APK infectados, que aparentan ser aplicaciones legítimas de gestión de relaciones con empleados y clientes (CRM).

Además, estas aplicaciones dropper usan técnicas como la manipulación de archivos ZIP para evitar ser detectadas y eludir las defensas de seguridad. Las víctimas son invitadas a registrarse en una cuenta y, posteriormente, se les solicita instalar una *«actualización de seguridad»* para mantener su dispositivo protegido. Asimismo, se les instruye para habilitar la instalación de aplicaciones desde fuentes desconocidas.

> *«Al hacer clic en el botón de 'Actualizar', aparece un ícono falso de Google Play Store que desencadena la instalación del malware»,* explicó Pratapagiri.
>
> *«Este programa malicioso solicita permisos de Servicios de Accesibilidad, que luego utiliza para superponer pantallas en el dispositivo y llevar a cabo acciones dañinas, como otorgarse permisos adicionales para ejecutar otras actividades maliciosas».*

La versión más reciente de Antidot incluye nuevas funciones que permiten a los operadores ejecutar configuraciones de *«Teclado e Introducción»*, interactuar con la pantalla de bloqueo dependiendo del método de seguridad configurado (PIN, patrón o contraseña), encender el dispositivo, reducir el brillo de la pantalla al mínimo, superponer páginas falsas para robar credenciales de cuentas de Google y prevenir su desinstalación.

También puede ocultar mensajes SMS específicos, bloquear llamadas de ciertos números predefinidos por un servidor remoto, abrir configuraciones de *«Aplicaciones predeterminadas»* y mostrar páginas falsas de inicio de sesión para 172 bancos, monederos de criptomonedas y plataformas como Facebook y Telegram.

Otras características del malware incluyen el registro de teclas (keylogging), el desvío de llamadas, el robo de mensajes SMS y la capacidad de usar Computación en Red Virtual (VNC)

para interactuar de forma remota con los dispositivos comprometidos.

Los principales objetivos de esta campaña son usuarios que hablen inglés, español, francés, alemán, italiano, portugués o ruso.

> *«Debido a las avanzadas capacidades del malware y al control casi total que puede ejercer sobre los dispositivos infectados, es crucial implementar medidas de seguridad preventivas y sólidas para proteger tanto a los usuarios como a sus dispositivos, evitando pérdidas de datos o financieras».*

Paralelamente, Cyfirma ha informado que activos valiosos en el sur de Asia han sido blanco de una campaña de malware para Android que distribuye el troyano SpyNote. Hasta el momento, estos ataques no han sido atribuidos a ningún grupo o actor específico.

> *«El uso recurrente de SpyNote es significativo, ya que demuestra la preferencia de los actores de amenazas por explotar esta herramienta para atacar a individuos de alto perfil, a pesar de que está disponible públicamente en foros clandestinos y canales de Telegram»,* concluyó la compañía.