Investigadores de ciberseguridad descubrieron aplicaciones fraudulentas en la tienda oficial Google Play Store para Android que afirmaban falsamente ofrecer acceso al historial de llamadas de cualquier número telefónico, cuando en realidad engañaban a los usuarios para que contrataran suscripciones que entregaban datos falsos y provocaban pérdidas económicas.

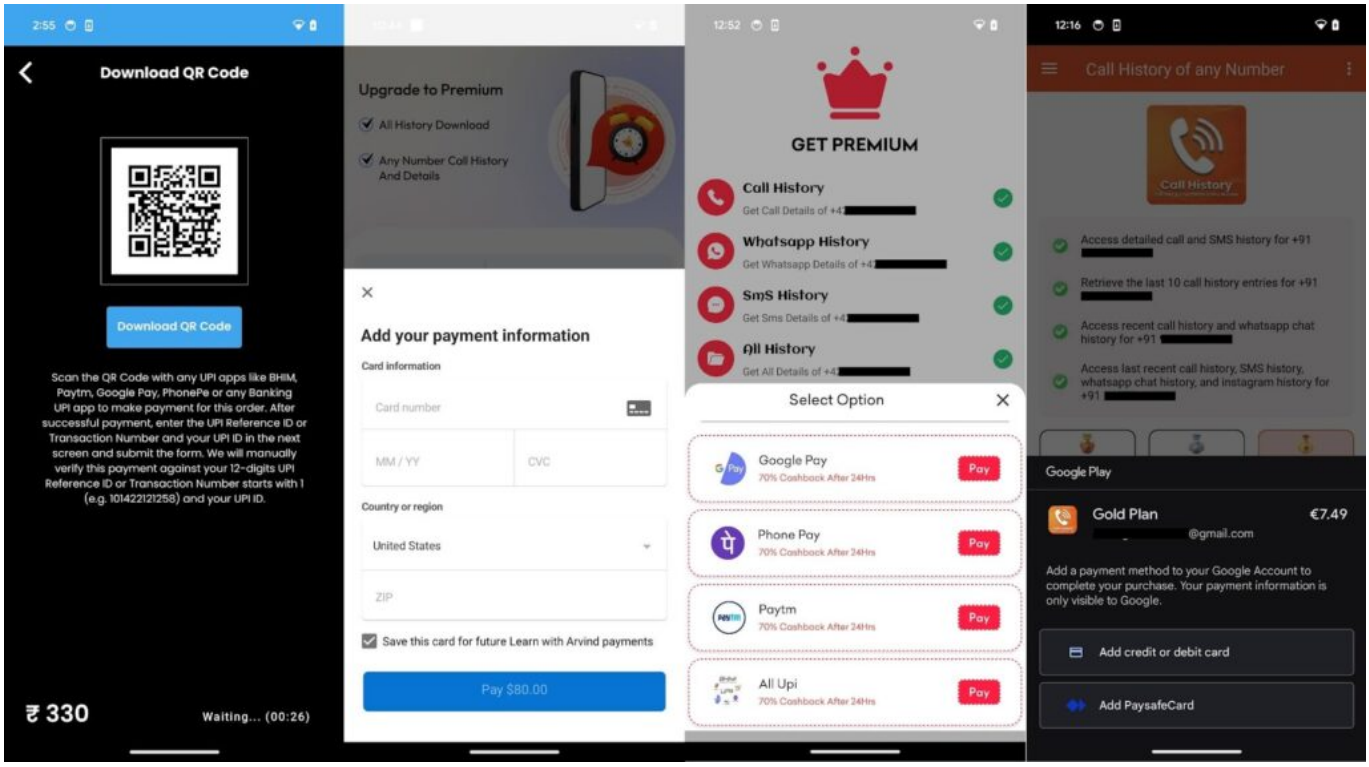
Las 28 aplicaciones acumularon más de 7.3 millones de descargas antes de ser eliminadas de la tienda oficial, y una sola de ellas superó los 3 millones de instalaciones. La operación, identificada con el nombre de *CallPhantom* por la empresa eslovaca de ciberseguridad ESET, estuvo dirigida principalmente a usuarios Android en India y otras regiones de Asia-Pacífico.

«Las aplicaciones involucradas, a las que denominamos CallPhantom debido a sus afirmaciones engañosas, aseguraban brindar acceso a historiales de llamadas, registros SMS e incluso registros de llamadas de WhatsApp de cualquier número telefónico», explicó el investigador de seguridad de ESET, Lukáš Štefanko, en un informe. *«Para desbloquear esta supuesta función, se solicitaba un pago a los usuarios, pero lo único que recibían eran datos generados aleatoriamente.»*

La lista de aplicaciones identificadas es la siguiente:

- *Call history : any number deta* (calldetaila.ndcallhisto.rytogetan.ynumber)
- *Call History of Any Number* (com.pixelxinnovation.manager)
- *Call Details of Any Number* (com.app.call.detail.history)
- *Call History Any Number Detail* (sc.call.ofany.mobiledetail)
- *Call History Any Number Detail* (com.cddhaduk.callerid.block.contact)
- *Call History Of Any Number* (com.basehistory.historydownloading)
- *Call History of Any Numbers* (com.call.of.any.number)
- *Call History Of Any Number* (com.rajni.callhistory)
- *Call History Any Number Detail* (com.callhistory.calldetails.callerids.callerhistory.callhostoryanynumber.getcall.history.callhistorymanager)
- *Call History Any Number Detail*

(com.callinformative.instantcallhistory.callhistorybluethem.callinfo)
- *Call History Any Number detail* (com.call.detail.caller.history)
- *Call History Any Number Detail* (com.anycallinformation.datadetailswho.callinfo.numberfinder)
- *Call History Any Number Detail* (com.callhistory.callhistoryyourgf)
- *Call History Any Number* (com.calldetails.smshistory.callhistoryofanynumber)
- *Call History Any Number Detail* (com.callhistory.anynumber.chapfvor.history)
- *Call History of Any Number* (com.callhistory.callhistoryany.call)
- *Call History Any Number Detail* (com.name.factor)
- *Call History Of Any Number* (com.getanynumberofcallhistory.callhistoryofanynumber.findcalldetailsofanynumber)
- *Call History Of Any Number* (com.chdev.callhistory)
- *Phone Call History Tracker* (com.phone.call.history.tracke)
- *Call History- Any Number Deta* (com.pdf.maker.pdfreader.pdfscanner)
- *Call History Of Any Number* (com.any.numbers.calls.history)
- *Call History Any Number Detail* (com.callapp.historyero)
- *Call History – Any Number Data* (all.callhistory.detail)
- *Call History For Any Number* (com.easyranktools.callhistoryforanynumber)
- *Call History of Numbers* (com.sbpinfotech.findlocationofanynumber)
- *Call History of Any Number* (callhistoryeditor.callhistory.numberdetails.calleridlocator)
- *Call History Pro* (com.all_historydownload.anynumber.callhistorybackup)



Al menos una de las aplicaciones señaladas fue publicada bajo el nombre de desarrollador *"Indian gov.in"*, con el objetivo de aparentar legitimidad y convencer a usuarios desprevenidos de descargarla.

Sin embargo, detrás de esta fachada existía un propósito malicioso: las víctimas debían realizar un pago para supuestamente acceder al historial de llamadas y mensajes SMS de un número telefónico. Después de pagar, los usuarios recibían números y nombres completamente inventados, integrados directamente en el código fuente de la aplicación. Las evidencias sugieren que esta operación podría haber estado activa desde noviembre de 2025.

Un segundo grupo de aplicaciones detectadas solicitaba a los usuarios ingresar su correo electrónico, prometiendo enviar allí los supuestos detalles del número consultado. Igual que en el caso anterior, no se generaba ninguna información hasta que se realizaba el pago.

Los cobros se realizaban mediante suscripciones usando el sistema oficial de facturación de Google Play Store o a través de aplicaciones externas compatibles con *Unified Payments Interface (UPI)*, un sistema de pagos instantáneos ampliamente utilizado en India. Entre estas plataformas se encontraban Google Pay, PhonePe y Paytm. Un tercer mecanismo consistía en formularios de pago con tarjeta directamente integrados en las aplicaciones, práctica que infringe las políticas de Google.

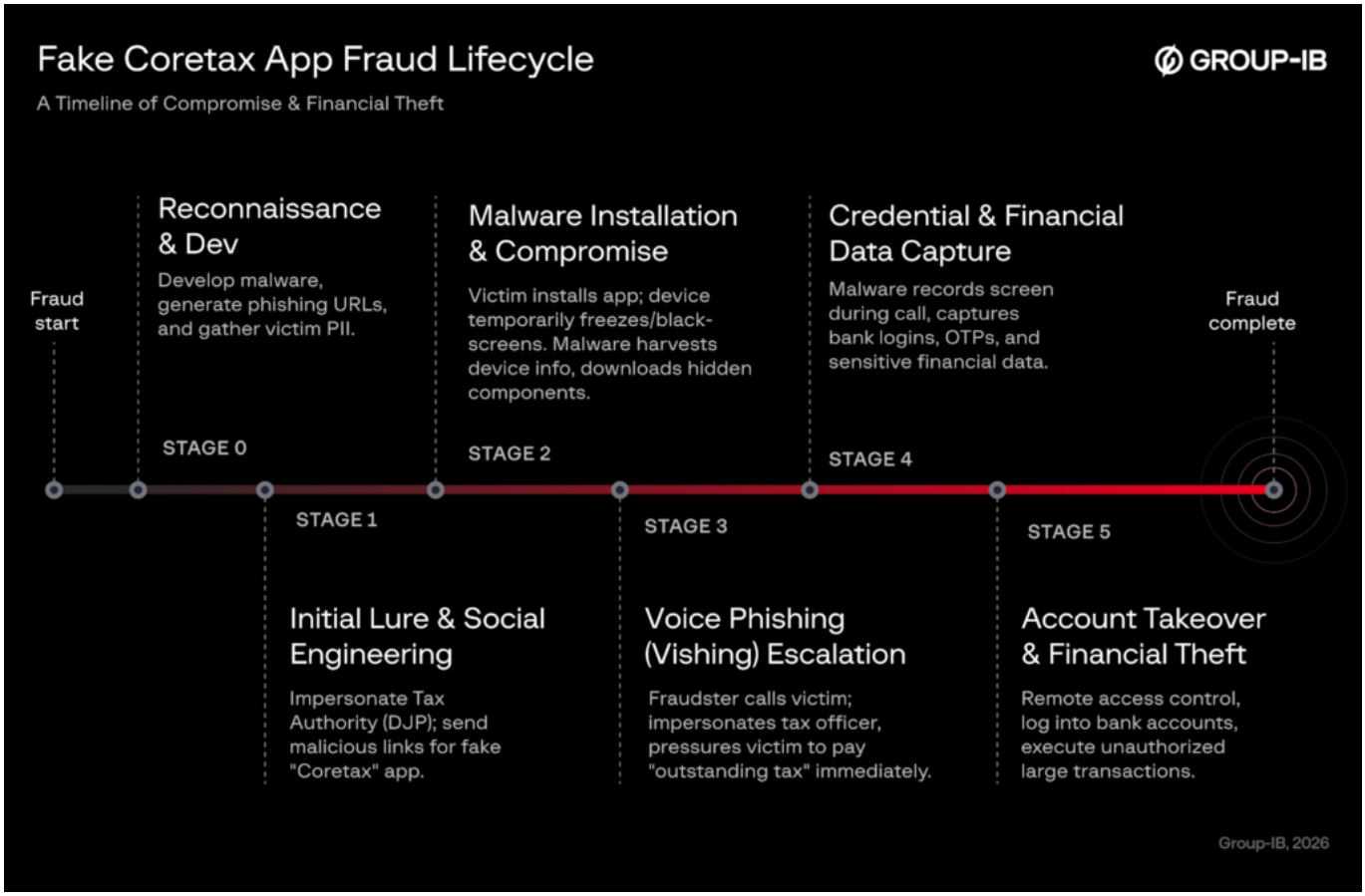
En al menos un caso, las aplicaciones implementaban una táctica adicional para presionar a los usuarios a pagar. Si la persona cerraba la aplicación sin realizar ningún abono, aparecía una notificación engañosa indicando que el historial de llamadas de cierto número había sido enviado exitosamente a su correo electrónico. Al pulsar sobre la notificación, el usuario era redirigido automáticamente a la pantalla de suscripción.

Los planes de suscripción variaban según la aplicación y oscilaban entre aproximadamente 6 y 80 dólares. Los usuarios afectados por la estafa probablemente tuvieron sus suscripciones canceladas tras la eliminación de las aplicaciones de la tienda oficial de Google.

Lo más llamativo de esta campaña es que las aplicaciones contaban con interfaces muy simples y no solicitaban permisos sensibles. Además, ni siquiera incluían funciones reales para obtener datos de llamadas, SMS o información de WhatsApp.

«Los usuarios que se suscribieron mediante el sistema oficial de pagos de Google Play podrían tener derecho a reembolsos conforme a las políticas de Google», señaló ESET. *«Las compras realizadas mediante aplicaciones de pago externas o formularios directos con tarjeta no pueden ser reembolsadas por Google, dejando a los usuarios dependiendo de proveedores externos o de los propios desarrolladores.»*

La revelación coincide con otro informe de la empresa de seguridad Group-IB, que afirmó que ciberdelincuentes robaron cerca de 2 millones de dólares a usuarios en Indonesia mediante una campaña de fraude que suplantaba la plataforma tributaria *CoreTax* y otras marcas confiables. La operación, iniciada en julio de 2025, fue vinculada a un grupo de amenazas con motivaciones financieras denominado *GoldFactory*.



«La cadena de ataque integra sitios web de phishing, ingeniería social a través de WhatsApp, instalación lateral de APK maliciosos y ataques de voz fraudulentos (vishing) para lograr el control total del dispositivo y ejecutar transferencias no autorizadas», explicó Group-IB.

A grandes rasgos, estos ataques utilizan técnicas de ingeniería social para distribuir aplicaciones falsas mediante WhatsApp. Una vez instaladas, despliegan malware Android como *Gigabud RAT*, *MMRat* y *Taotie*, capaces de robar información sensible y descargar componentes adicionales. Los datos obtenidos posteriormente se utilizan para secuestrar cuentas y realizar fraudes financieros.

«La infraestructura maliciosa detrás de esta campaña no se limita a un único servicio suplantado. Se ha observado el abuso activo de más de 16 marcas confiables, afectando

potencialmente a la población de Indonesia, que supera los 287 millones de habitantes», concluyó Group-IB.