Alerta

Técnica

Campañas de "Retorno Operativo"

COLCERT AL - 20260123 - 090

TLP:CLEAR

Resumen Ejecutivo

Panorama General

El inicio del calendario tributario 2026 ha activado una campaña de ciberataques dirigida a empresas y ciudadanos que realizan trámites de renovación de matrícula mercantil y actualización de RUT.

Los criminales han evolucionado hacia un modelo híbrido: utilizan Inteligencia Artificial para clonar la voz de funcionarios o directivos (DeepVoice/Vishing) para generar una falsa sensación de urgencia, y la combinan con códigos QR maliciosos (Quishing) para evadir los filtros de seguridad del correo electrónico corporativo. El objetivo final es el robo de credenciales bancarias y el acceso silencioso a redes corporativas.

NIVEL DE RIESGO

ALTO

⚠️ **La premisa del ataque:** ***Si recibes una llamada urgente sobre un "bloqueo de firma digital" o "sanción inminente" seguida de un correo con un QR para solucionarlo, es una trampa.*** ⚠️

Evidencia y contexto

Validación oficial

Esta alerta se fundamenta en tendencias criminales confirmadas por el Centro Cibernético Policial en su Balance Anual 2025, el cual arroja las siguientes evidencias irrefutables:

- **El Crimen Financiero es la Amenaza #1:** Contrario a la disminución de otros delitos, el "Hurto por medios informáticos" presentó un incremento del 4% en el último año, consolidándose como el delito de mayor impacto con 38.946 casos reportados. Esto confirma que los atacantes priorizan la sustracción de activos.

- **Vishing y Phishing Activos (Caso "Resident"):** Las autoridades confirmaron la operatividad de bandas dedicadas a la ingeniería social telefónica. En la Operación Resident, se capturó a una organización que utilizaba modalidades de vishing y phishing para obtener datos personales, afectando a más de 1.123 víctimas con un detrimento patrimonial superior a los 3.000 millones de pesos.

- **El reporte oficializa la detección del "Uso criminal de Inteligencia Artificial (IA)",** específicamente la modalidad DeepFake, para crear contenido de audio y video manipulado que parece real, facilitando la suplantación de identidad.

- Se insta a extremar medidas en Bogotá, Medellín y Cali, ciudades que, junto con otras tres capitales, concentran el 50% de la afectación nacional.

Análisis técnico

Para Equipos de TI, SOC y CSIRT

Vector de Ataque: Híbrido (Voz + QR + Malware Fileless)

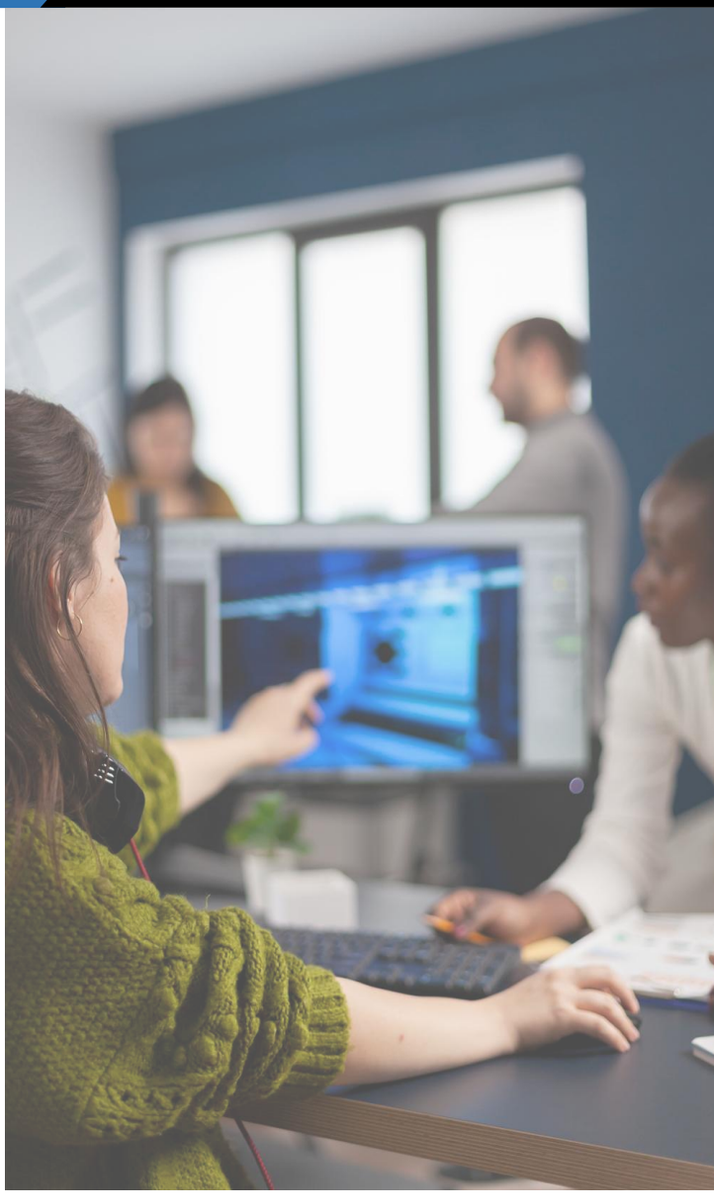
- **Ingeniería Social (Vishing con IA):** El atacante usa herramientas de clonación de voz para suplantar a un ente de control (DIAN/Cámara de Comercio) o un directivo (CEO Fraud).
- **Evasión de Perímetro (Quishing):** Envío de un correo electrónico que contiene solo una imagen QR. Los Secure Email Gateways (SEG) tradicionales a menudo no renderizan ni escanean la imagen, permitiendo que el phishing llegue al buzón del usuario.

Ejecución (Loader Polimórfico):

- Al escanear el QR, el dispositivo (móvil o PC) descarga un script ofuscado.
- Este script conecta a un servidor de Comando y Control (C2) para descargar el payload final directamente en la memoria RAM (Fileless), evitando escribir en el disco duro para evadir antivirus tradicionales.

Indicadores de Compromiso (IoCs) y Detección:

- Monitoree procesos de ofimática lanzando powershell.exe con parámetros como -WindowStyle Hidden o -EncodedCommand.
- Esté alerta a dominios que imitan portales bancarios o gubernamentales. En 2025 se reportaron 3.896 casos de suplantación de sitios web, técnica clave en este esquema.



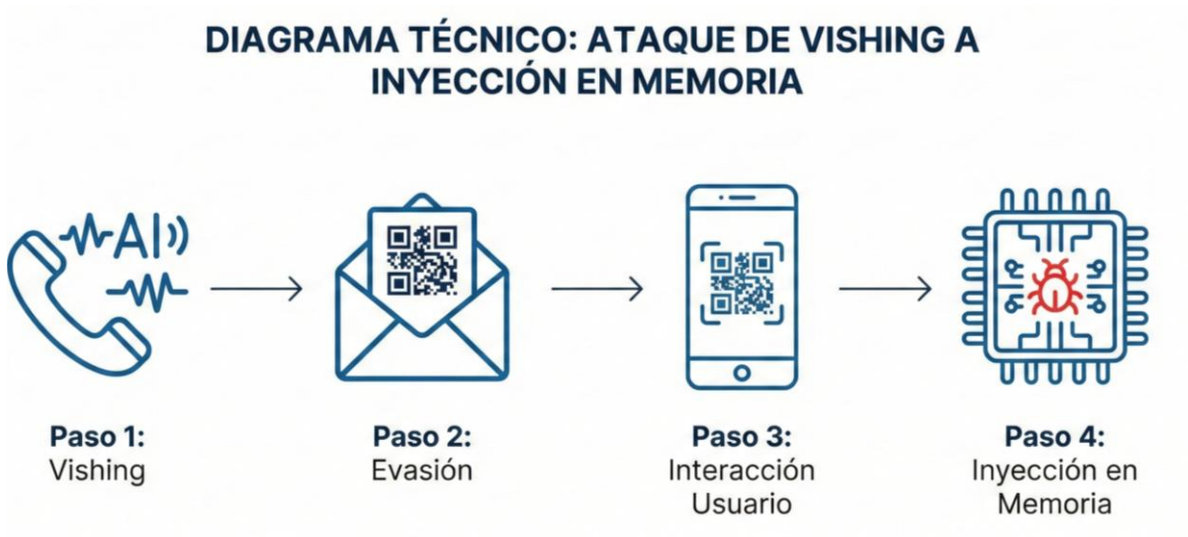


Figura 1: *Cadena de infección híbrida. Diagrama de flujo que ilustra la secuencia de ataque, desde la ingeniería social por voz (Vishing) hasta la evasión de filtros mediante QR y la posterior inyección de código en memoria.*

Recomendaciones de inicio de año

Para la ciudadanía y empleados

- Si recibe una llamada inusual solicitando acciones urgentes, cuelgue. Llame usted mismo al número oficial de la entidad. La voz ya no garantiza la identidad.
- No escanee códigos QR enviados por correo electrónico para "actualizar datos". Digite manualmente la dirección web de la entidad en su navegador.

Para administradores de sistemas (Hardening)

- Habilite el Script Block Logging (Evento 4104) en PowerShell. Es la defensa más efectiva para visualizar el código que los atacantes intentan ejecutar en memoria.
- Migre a autenticación multifactor (MFA) física (FIDO2) para administradores, ya que el MFA por SMS es vulnerable a estas campañas de ingeniería social.

Glosario técnico

- **Vishing (Voice Phishing):** Estafa telefónica donde el atacante usa ingeniería social (y ahora IA) para engañar a la víctima mediante la voz.
- **Quishing (QR Phishing):** Ataque que utiliza códigos QR para ocultar enlaces maliciosos, evadiendo los filtros de seguridad de correo electrónico tradicionales.
- **DeepVoice / Audio Deepfake:** Uso de Inteligencia Artificial para crear audios sintéticos que imitan la voz de una persona real, diciendo cosas que nunca ocurrieron.
- **Loader Polimórfico:** Malware que cambia su código interno cada vez que se descarga para evitar ser reconocido por los antivirus.
- **Fileless Malware:** Software malicioso que opera únicamente en la memoria del computador, sin guardar archivos en el disco duro.

Fuentes

- Policía Nacional de Colombia - Dirección de Investigación Criminal e INTERPOL (DIJIN): "Balance Anual 2025 - Centro Cibernético Policial". Documento base para estadísticas nacionales y casos operativos (Operación Resident).
- ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia): Reportes de monitoreo de campañas activas en el ciberespacio nacional (Enero 2026).
- Inteligencia de Amenazas Global: Referencias a tácticas TTPs (Tácticas, Técnicas y Procedimientos) observadas en casos internacionales de fraude financiero vía Deepfake (Caso Hong Kong 2024).