Boletín de Ciberseguridad

Phishing especializado

Actividad del grupo APT-C-36

TIC

Instituto Nacional de Cancerología Colombia
Por el control del cáncer

Resumen Ejecutivo

En Colombia se ha identificado actividad reciente del grupo de ciberamenazas **APT-C-36**, también conocido como ***Blind Eagle***. Este grupo realiza **campañas de correos falsos** (phishing) diseñados para engañar a funcionarios y ciudadanos, con el fin de instalar programas maliciosos que permiten tomar control de los equipos.

Sus ataques se enfocan especialmente en instituciones públicas, como la DIAN, la Rama Judicial, la Fiscalía General de la Nación y otras instituciones oficiales

---

🧐 ¿Quién es APT-C-36?

APT-C-36 es un grupo de ciberdelincuencia activo desde al menos 2018. Se caracteriza por:

- Dirigir sus ataques a **Colombia y otros países de Latinoamérica**.
- Suplantar entidades oficiales como la **DIAN, Fiscalía, Rama Judicial** o **Centro Cibernético Policial**.
- Enviar correos que aparentan ser notificaciones urgentes (procesos legales, citaciones, cobros, etc.).
- Buscar que la víctima haga clic en enlaces o adjuntos para instalar malware y robar información.

Este grupo se especializa en entender la burocracia colombiana, lo que hace que sus mensajes parezcan **auténticos y muy convincentes**.

✉️ ¿Cómo engañan a las víctimas?

El proceso suele seguir estos pasos:

1. **Investigación previa:** El grupo identifica correos institucionales y estudia los procesos administrativos para hacer mensajes creíbles.
2. **Creación de correos falsos:** Los mensajes imitan documentos oficiales como facturas, citaciones o notificaciones.
3. **Entrega del mensaje:** La víctima recibe un correo con un botón, enlace o archivo aparentemente legítimo.
4. **Interacción del usuario:** Al hacer clic, se descargan archivos desde páginas controladas por los atacantes.
5. **Instalación del malware:** Se instala un programa que permite al atacante controlar el equipo de manera remota.
6. **Conexión con el servidor del atacante:** El malware se comunica con un centro de comando mediante internet, donde los delincuentes pueden robar información o ejecutar acciones adicionales.

🏥 ¿Por qué es relevante para el Instituto Nacional de Cancerología?

Al ser una entidad que maneja información sensible de pacientes, procesos administrativos y comunicaciones oficiales, el INC es un posible objetivo para este tipo de campañas de phishing.

Los atacantes pueden buscar:

- Robar credenciales de acceso.
- Ingresar a sistemas institucionales.
- Acceder a datos de pacientes.
- Afectar procesos asistenciales o administrativos.

Vector de Ataque

El vector de ataque predominante se basa en la suplantación de identidad de entidades estatales, generando una sensación de urgencia en la víctima, se han identificado campañas masivas suplantando a:

- **DIAN (Dirección de Impuestos y Aduanas Nacionales):** correos sobre supuestos "procesos de cobro coactivo", "embargos de cuentas bancarias" o "facturación electrónica obligatoria". Es la temática más recurrente debido a su impacto directo sobre empresas y ciudadanos.

Imagen 1. *Suplantación de la DIAN.* ***Fuente:*** *ColCERT.*

- **Rama Judicial y Fiscalía General de la Nación:** notificaciones falsas de "citaciones a audiencia", "demandas en curso" o "apertura de procesos penales". Estos señuelos suelen incluir supuestos enlaces a expedientes digitales.

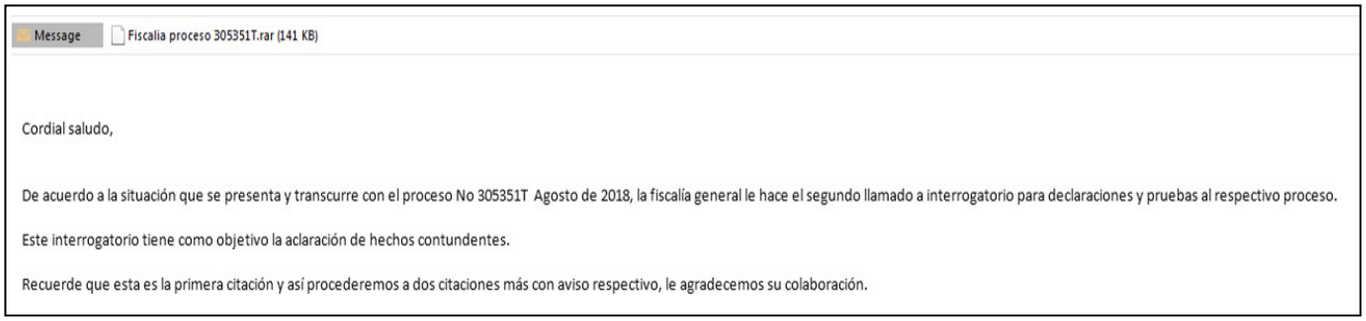

Imagen 2. *Suplantación de la Fiscalía General de la Nación.* ***Fuente:*** *ColCERT.*

- **Centro Cibernético Policial y Cancillería:** en menor medida, se han detectado campañas relacionadas con antecedentes judiciales o trámites de pasaportes.

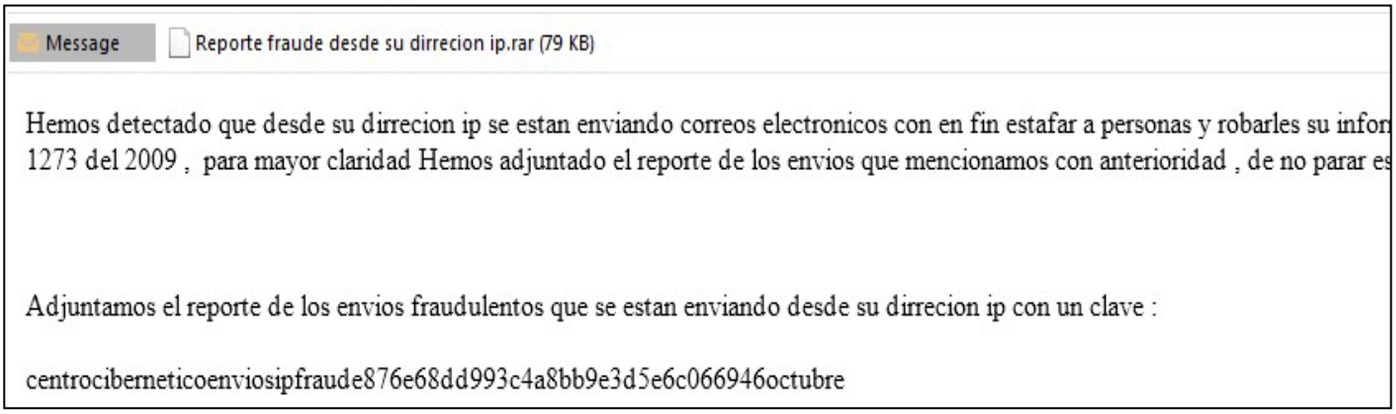

Imagen 3. *Suplantación del Centro Cibernético Policial.* ***Fuente:*** *ColCERT.*

⚠️ Tipos de archivos o enlaces maliciosos utilizados

APT-C-36 usa diferentes mecanismos, entre ellos:

- Enlaces que llevan a páginas maliciosas, incluso alojadas en servicios legítimos (nube, repositorios).
- Archivos tipo HTML o SVG que redirigen o descargan malware.
- Documentos con macros que ejecutan código peligroso.
- Archivos disfrazados, como supuestos PDF que realmente son programas ejecutables.
- Imágenes con información oculta (esteganografía) que contienen partes del malware.

🔐 Recomendaciones principales para el INC

Para reducir riesgos, se recomienda:

- Evite abrir correos con mensajes de urgencia exagerada.
- Verifique siempre el remitente.
- No descargue archivos ni haga clic en enlaces de dudosa procedencia.
- Recuerde que entidades como la DIAN, Fiscalía o bancos rara vez envían enlaces directos a documentos sensibles.

🧭 Conclusión

APT-C-36 es un grupo especializado que continúa representando una amenaza significativa para entidades públicas en Colombia. Su capacidad para crear correos convincentes aumenta el riesgo de infección si no se toman medidas preventivas.

La mejor defensa es una combinación de:

- **Seguridad tecnológica robusta**,
- **Monitoreo constante**, y
- **Personal capacitado y alerta**.