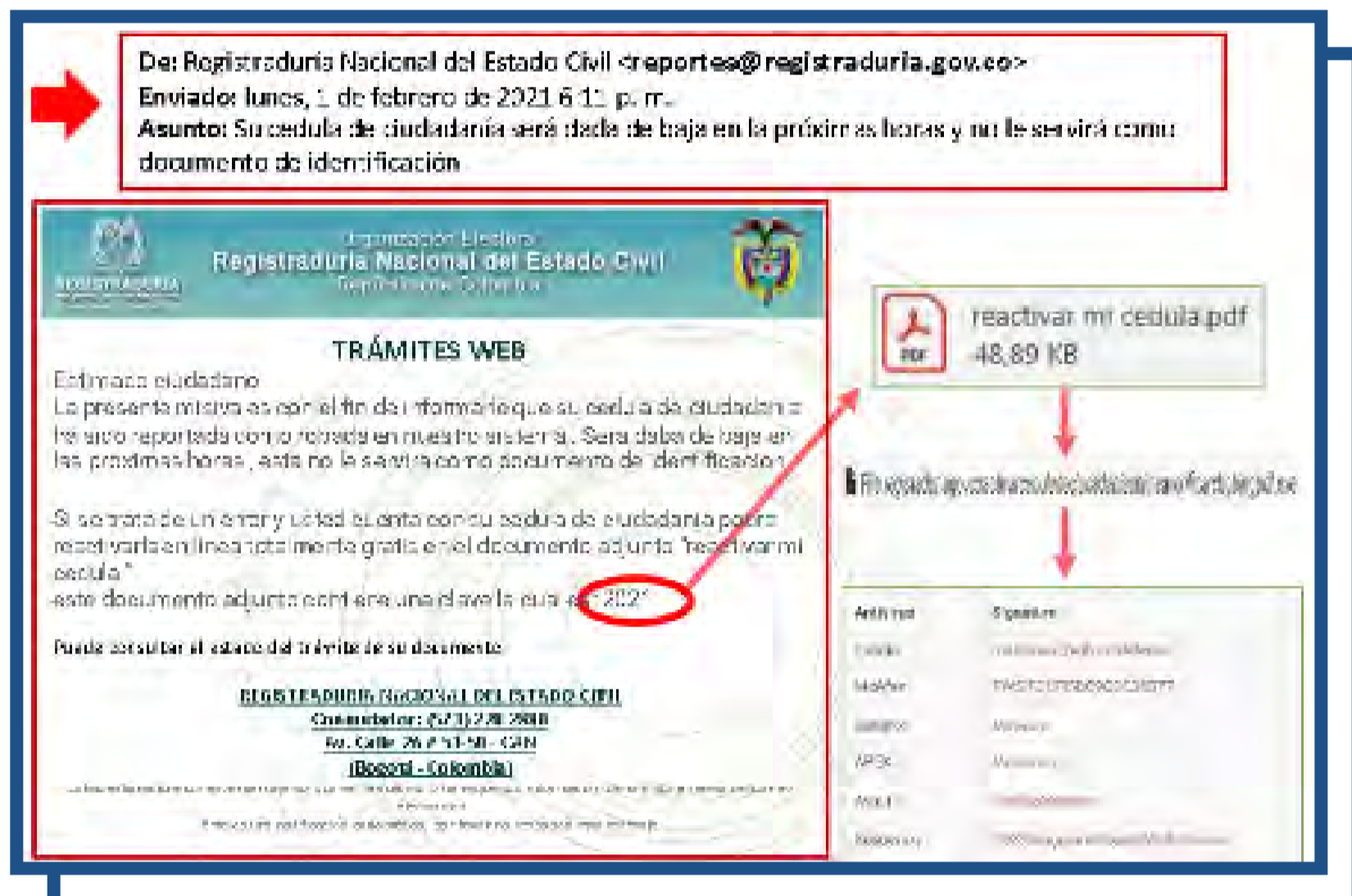


## Nueva estrategia de extracción de información para fines delictivos

### ¡MALWARE CIRCULANDO EN LA RED!

Se reportan **múltiples eventos de suplantación de identidad a la Registraduría Nacional** acompañados de campañas de SPAM, donde los delincuentes buscan engañar al ciudadano mediante una **falsa alerta sobre la baja del documento de indentificación**, en la cual se informa que la **Cédula de Ciudadanía se reportó como robada** motivo por el cual después de un tiempo no será un documento válido, con el objetivo que la **víctima ingrese al link enunciado o descargue el archivo infectado, y así poder extraer información para fines delictivos, infectar equipos con códigos maliciosos, ramsonware, malware, virus informáticos u otros propósitos.**



#### VERIFICA CON ATENCIÓN:

El mensaje del correo no tiene tildes ni justificación y el logo de la Registraduría Nacional no es el actual.

### Reconoce terminología:

**Campaña de spam:** envíos masivos de correos maliciosos o malintencionados con el propósito de extraer información, causar molestia o infectar con virus los equipos.

**Ransomware:** Tipo de malware que secuestra la información y exige un pago para el rescate de esta.



Para evitar ser víctima de alguno de los crímenes mencionados anteriormente, toma en cuenta las siguientes **recomendaciones:**

- **No ingresar a links** o enlaces que estén dentro de correos desconocidos o sospechosos.
- **No descargar o abrir archivos adjuntos** de correos desconocidos y sospechosos.
- **No diligenciar formularios que estén anexos** a los mensajes sospechosos.
- **No responder mensajes que soliciten información personal o financiera** (usuarios, cédula, fecha de nacimiento, contraseñas, etc.).
- Para los equipos personales, **mantenga actualizado el sistema operativo y antivirus.**
- **Verificar la ortografía y redacción del correo**, ya que en ocasiones los correos maliciosos no tienen congruencia en la redacción o tienen errores ortográficos.
- **Sospechar de los correos genéricos**, por ejemplo:
  - o Estimado ciudadano.
  - o Señor(a)
  - o Estimados.
  - o Etc.
- **Para validar que una URL o el archivo es legítima puede utilizar las siguientes herramientas online:**
  - o <https://cc-csirt.policia.gov.co/Sandbox>
  - o <https://www.virustotal.com/gui/home/url>
  - o <https://www.urlvoid.com/>