Nro. Alerta:	AL-2026-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	08-may-26	**Suplantación de Identidad "Ministerio de Inclusión Económica y Social - MIES"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude digital / Ingeniería social

Tipo de incidente: Suplantación de identidad (phishing) mediante sitio web fraudulento y propagación por mensajería instantánea (WhatsApp), con posible distribución de malware.

Nivel de riesgo: Alto — debido a la recolección de datos personales sensibles, alta capacidad de propagación, suplantación de entidad gubernamental y riesgo de compromiso de cuentas y dispositivos.

II. INTRODUCCIÓN

El fraude es una acción ilegal en la que una persona o grupo engaña a otros con el fin de obtener dinero, información personal u otros beneficios de manera indebida. Generalmente, se basa en mentiras, promesas falsas o suplantación de identidad para generar confianza en la víctima. Este tipo de actos no solo causa pérdidas económicas, sino también afecta la seguridad y tranquilidad de quienes son engañados.

En particular, existe una modalidad de fraude en la que los atacantes se hacen pasar por entidades gubernamentales o aseguran representar programas oficiales. En estos casos, ofrecen supuestos beneficios económicos, bonos, subsidios o ayudas del gobierno, con el objetivo de convencer a las personas de que entreguen datos personales, números de cuentas bancarias o incluso realicen pagos "para acceder" a dichos beneficios. Estas ofertas suelen difundirse a través de mensajes de texto, redes sociales, correos electrónicos o llamadas telefónicas.

Es importante tener en cuenta que las instituciones gubernamentales no solicitan pagos para otorgar beneficios ni piden información sensible por medios informales. Por ello, se recomienda verificar siempre la autenticidad de cualquier anuncio en canales oficiales, no compartir datos personales con desconocidos y desconfiar de mensajes que prometen dinero fácil o urgente. La prevención y la información son claves para evitar caer en este tipo de fraude.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	08-may-26	**Suplantación de Identidad "Ministerio de Inclusión Económica y Social - MIES"**	V 1.1

III. VECTOR DE ATAQUE:

1. **Suplantación mediante sitio web móvil.**

   Los atacantes crean una página web fraudulenta que suplanta la identidad del extinto Ministerio de Inclusión Económica y Social (MIES), promocionando un supuesto bono de 750 dólares por el Día de la Madre. Este sitio está diseñado para mostrarse únicamente en dispositivos móviles, lo que dificulta su detección desde computadoras de escritorio y aumenta la probabilidad de que los usuarios confíen en su autenticidad.

2. **Recolección de información personal.**

   La página solicita datos personales como número de cédula, situación laboral, estado civil y rango de edad. Esta recolección de información busca simular un proceso legítimo de validación, generando confianza en la víctima mientras los atacantes obtienen datos sensibles que pueden ser utilizados en fraudes posteriores o suplantación de identidad.

3. **Propagación mediante WhatsApp y manipulación social.**

   Tras completar el formulario, se informa a la víctima que su solicitud ha sido aprobada. Como siguiente paso, se le indica que debe compartir la promoción a través de WhatsApp con 10 contactos o 5 grupos. El sitio incorpora una barra de progreso que se llena conforme se realizan los envíos, creando una sensación de avance real y presionando al usuario a cumplir con la acción. Este mecanismo permite que el fraude se propague rápidamente a nuevas víctimas.

4. **Riesgo de compromiso del dispositivo o cuenta.**

   Una vez completado el proceso, se promete la entrega de un código para acceder al bono, manteniendo a la víctima involucrada hasta la etapa final del engaño. En esta fase, el usuario puede ser redirigido a enlaces adicionales, solicitarle ingresar códigos de verificación recibidos por SMS o incluso inducirlo a descargar aplicaciones maliciosas fuera de tiendas oficiales. Estas acciones forman parte de técnicas diseñadas para tomar control parcial o total del dispositivo o de sus cuentas.

   Existe una alta probabilidad de secuestro de la cuenta de WhatsApp mediante la captura de códigos de verificación, lo que permite a los atacantes suplantar la identidad de la víctima y continuar propagando el fraude. Asimismo, puede

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

producirse la instalación de malware (como spyware, troyanos o aplicaciones con permisos abusivos) que permita el acceso a información sensible almacenada en el dispositivo, incluyendo contactos, mensajes, credenciales y archivos personales.

Adicionalmente, el compromiso del dispositivo puede derivar en monitoreo de actividad, robo de credenciales de otras aplicaciones (correo electrónico, banca móvil, redes sociales) y ejecución de acciones sin el consentimiento del usuario.

En escenarios más avanzados, los atacantes pueden utilizar la cuenta comprometida para solicitar dinero a los contactos de la víctima, simulando situaciones de emergencia o urgencia, lo que incrementa significativamente el impacto del incidente tanto a nivel individual como colectivo.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa son los enlaces que dirigen a los sitios web fraudulentos:

- ***Sitios web:***

  hxxps://aportefamiliar[.]info/consultar

  hxxps://aportefamiliar[.]info/consultar/2026/registro/step2.html#1778099724101

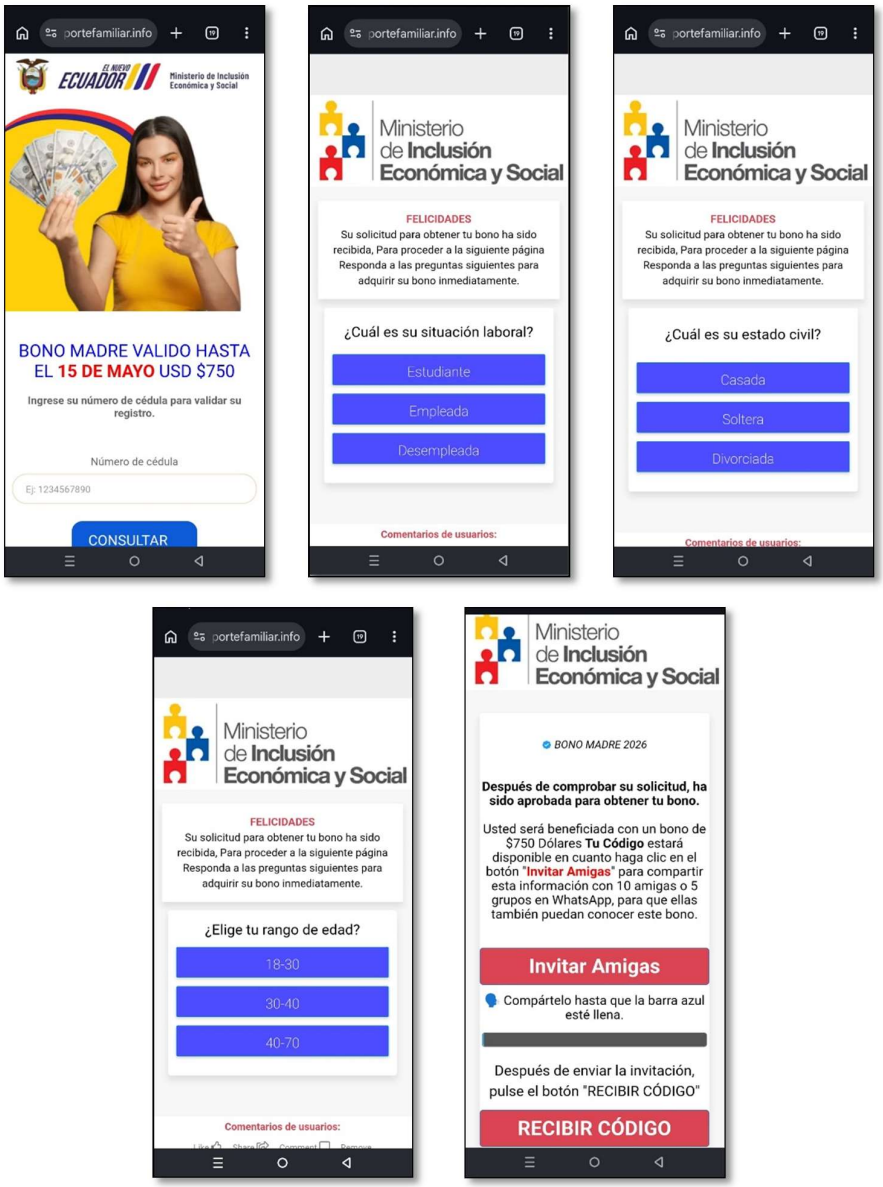
- ***Ip´s:***

  145.223.124.238 (*fuente virustotal.com*)

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	08-may-26	**Suplantación de Identidad "Ministerio de Inclusión Económica y Social - MIES"**	V 1.1



Gráfica 1.- Sitio web que suplanta al extinto Ministerio de Inclusión Económica y Social

VI. SITIO WEB REAL DEL MINISTERIO DE DESARROLLO HUMANO.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	08-may-26	**Suplantación de Identidad "Ministerio de Inclusión Económica y Social - MIES"**	V 1.1

El Ministerio de Desarrollo Humano del Ecuador (reemplazó y amplió funciones del anterior Ministerio de Inclusión Económica y Social en algunos procesos de reorganización estatal) se formó como parte de un proceso de reestructuración del Ejecutivo orientado a fortalecer la política social del país.

https://www.desarrollohumano.gob.ec/

Gráfica 2.- Información en Página WEB real del Ministerio de Desarrollo Humano.

VII. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Verificar siempre que los sitios web consultados sean oficiales de instituciones gubernamentales, revisando que el dominio corresponda a entidades legítimas del Estado y que utilicen conexiones seguras (https), evitando enlaces recibidos por redes sociales o mensajes no solicitados.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DE ARCOTEL **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	08-may-26	**Suplantación de Identidad "Ministerio de Inclusión Económica y Social - MIES"**	V 1.1

- Ignorar y no interactuar con mensajes, enlaces o publicaciones que ofrezcan bonos, premios o beneficios económicos no solicitados, especialmente si exigen compartir el contenido en WhatsApp o redes sociales.
- Confirmar cualquier información sobre bonos, ayudas o subsidios directamente en canales oficiales del Gobierno o contactando a la institución correspondiente, evitando depender de enlaces enviados por terceros.
- En caso de haber ingresado datos personales en una página sospechosa, realizar de inmediato acciones de protección como cambio de contraseñas, monitoreo de cuentas y notificación a las entidades oficiales para prevención de uso indebido de la información.
- Nunca proporcionar información personal, números de cédula, datos financieros o códigos de verificación en sitios web, formularios o mensajes no verificados, aunque estos aparenten provenir de instituciones públicas.
- Mantener actualizado el software de seguridad (antivirus/antimalware) en los dispositivos móviles, ya que estos pueden ayudar a detectar aplicaciones o archivos maliciosos asociados a este tipo de fraudes.
- Evitar la instalación de aplicaciones o archivos provenientes de enlaces enviados por mensajería instantánea o páginas no oficiales, incluyendo archivos .apk fuera de tiendas oficiales como Google Play Store o AppGallery.
- No compartir cadenas, promociones o enlaces de supuestos bonos en WhatsApp, ya que este mecanismo es utilizado para propagar el fraude entre contactos y aumentar su alcance.
- Mantenerse informado sobre nuevas modalidades de fraude digital para poder identificar señales de alerta como promesas de dinero fácil, urgencia o solicitudes de compartir contenido.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec