Nro. Alerta:	AL-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: App Fraud

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El fraude a través de aplicaciones móviles es una modalidad delictiva en la que los atacantes distribuyen aplicaciones aparentemente legítimas, pero que contienen código malicioso diseñado para comprometer la seguridad del usuario. Estas aplicaciones suelen ser promovidas mediante técnicas de ingeniería social, mensajes engañosos o enlaces fraudulentos, con el fin de inducir a la víctima a instalarlas en su dispositivo.

Una vez instalada, la aplicación maliciosa puede obtener permisos indebidos, capturar información sensible, interceptar comunicaciones (incluidos SMS y códigos de autenticación), acceder a credenciales bancarias o incluso tomar control remoto del dispositivo. El objetivo principal de este tipo de fraude es el robo de datos personales, credenciales de acceso o recursos financieros de la víctima.

Este tipo de ataques representa un riesgo significativo para la seguridad digital, por lo que se recomienda a los usuarios instalar aplicaciones únicamente desde tiendas oficiales, verificar los permisos solicitados, y desconfiar de enlaces recibidos por canales no verificados.

III. VECTOR DE ATAQUE:

Se ha detectado la circulación de un sitio web fraudulento que suplanta la identidad del extinto Ministerio del Trabajo, ofreciendo supuestas vacantes laborales.

El portal fraudulento utiliza logotipos oficiales, identidad gráfica similar a la institucional y lenguaje formal para generar confianza en la ciudadanía.

Los atacantes difunden el enlace del sitio fraudulento a través de: redes sociales, mensajes masivos por WhatsApp, grupos de Telegram, correos electrónicos tipo phishing y publicaciones patrocinadas falsas.

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-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

El mensaje publicado en el sitio web fraudulento se muestra como: "*EMPLEOS DISPONIBLES – Información de empleos disponibles 2026, solicite ahora*"

Una vez que la víctima accede al sitio fraudulento, se le solicita seleccionar la institución pública en la que desea aplicar, luego se requiere el ingreso de la siguiente información:

- Nombres y apellidos completos
- Número telefónico, el cual debe estar vinculado con la aplicación Telegram.

En esta etapa el objetivo principal es validar números activos, identificar usuarios con cuenta en Telegram y construir bases de datos para campañas posteriores

Una vez que el número es identificado como usuario activo en Telegram, los atacantes pueden:

a) Contacto directo desde cuentas falsas:

- Simulan ser personal de talento humano.
- Envían enlaces adicionales.
- Solicitan información complementaria (cédula, dirección, foto de documento).

b) Integración en grupos fraudulentos

- Agregan a la víctima a grupos que aparentan ser oficiales.
- Simulan procesos de selección.
- Publican testimonios falsos de "personas contratadas".

c) Solicitud de pagos: pueden exigir

- Pago por validación de documentos
- Costo de exámenes médicos
- Tasa administrativa
- Compra de uniforme o credenciales

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-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

Este es el punto donde se concreta la estafa económica.

d) Robo de identidad: Con los datos recolectados pueden:

- Crear perfiles falsos.
- Intentar suplantación digital.
- Ejecutar fraudes financieros.
- Realizar campañas de SIM swapping.

e) Envío de archivos maliciosos

- Documentos PDF con malware.
- APKs falsas de "aplicación institucional".
- Enlaces a sitios de credential harvesting (recolección de credenciales)

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:***

  https://trabajo.m1es-ec.com/#main

  https://trabajo.m1es-ec.com/signin

- ***Ip´s:***

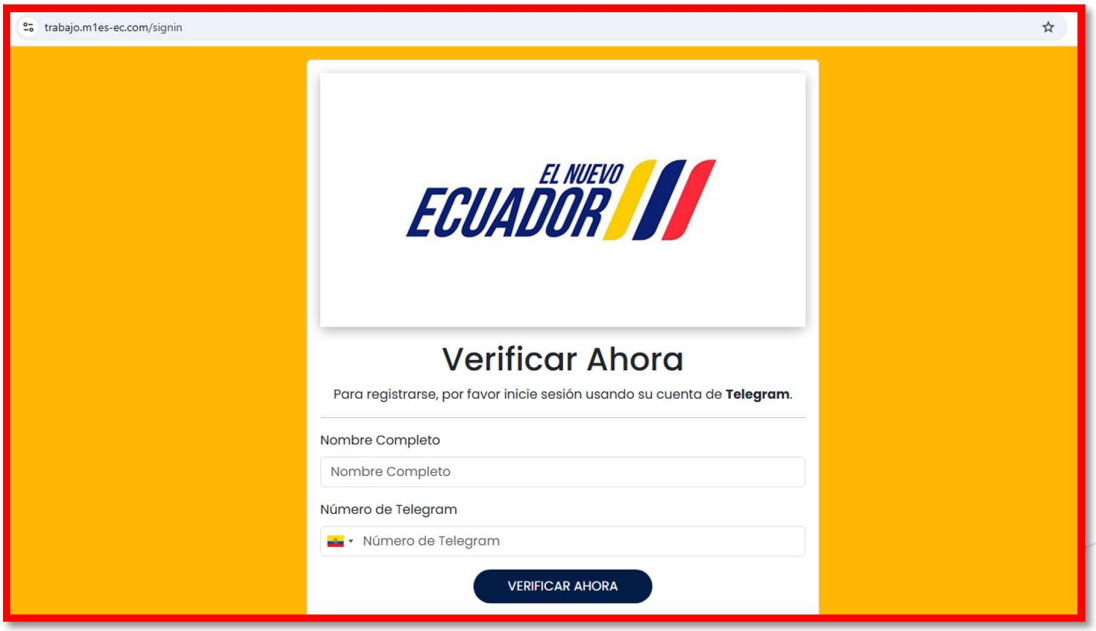
  103.16.117.244 (*fuente virustotal.com*)

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-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD.

Gráfica 1.- Sitio web que suplanta al Ministerio del Trabajo.



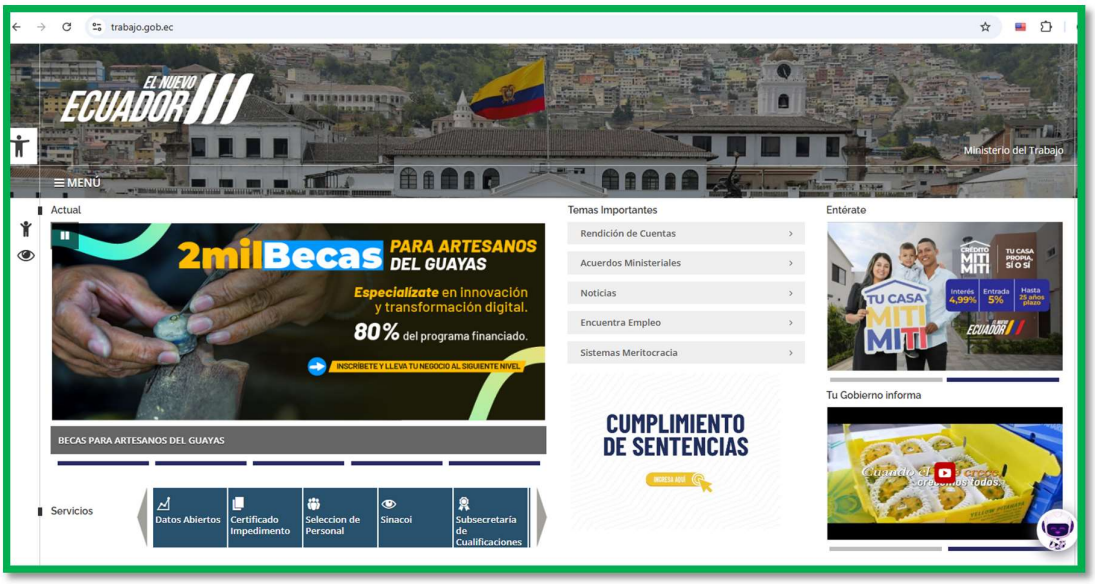
Gráfica 2.- Sitio web que suplanta al Ministerio del Trabajo, solicitando información personal.

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-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

VI. SITIO WEB REAL DEL MINISTERIO DEL TRABAJO.

https://www.trabajo.gob.ec/



Gráfica 3.- Información en Página WEB real del Ministerio del trabajo.

VII. RECOMENDACIONES:

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

- Validar si los sitios web en los que se navega son seguros (se utiliza el puerto https) y oficiales (el dominio corresponde al nombre de la empresa, no tiene errores ortográficos).
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- En caso de haber ingresado los datos personales en el sitio web fraudulento, cambiar la contraseña de las cuentas y comunicarse inmediatamente con la empresa suplantada para la toma de acciones de remediación.

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-2025-008	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	**Suplantación de Identidad "Ministerio del Trabajo"**	V 1.1

- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.
- Mantenerse informado continuamente sobre tipos de amenazas en el internet.
- Instalar archivos .apk en su dispositivo descargarlo sólo de fuentes confiables como Google Play Store, AppGallery, Galaxy Store u otras tiendas oficiales.

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