Nro. Alerta:	EC-2022-42	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-feb-2022	**EcuCERT advierte nueva campaña de pharming en "BANECUADOR"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Scam

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

Con el fin de obtener datos personales, especialmente usuario y contraseña de las cuentas bancarias virtuales, el ciberdelincuente redirige el tráfico web del usuario a un sitio creado y manejado por él; es decir, se suplanta un sitio web auténtico por otro falso. Este ciberdelito es conocido como pharming.

III. VECTOR DE ATAQUE:

A través de búsquedas en internet, se encuentra disponible un sitio web malicioso que suplanta la identidad de la página web del BanEcuador, el sitio web que simula ser el real, engaña a la víctima para que ingrese su usuario y contraseña de la banca digital.

IV. INDICADORES DE COMPROMISO:

A continuación, el indicador de compromiso asociado a la campaña maliciosa:

- https://enlineaecuador[.]store/5/IndexBanEcuador[.]html

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-42	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-feb-2022	**EcuCERT advierte nueva campaña de pharming en "BANECUADOR"**	V 1.1

V. IMAGEN DE LA CAMPAÑA

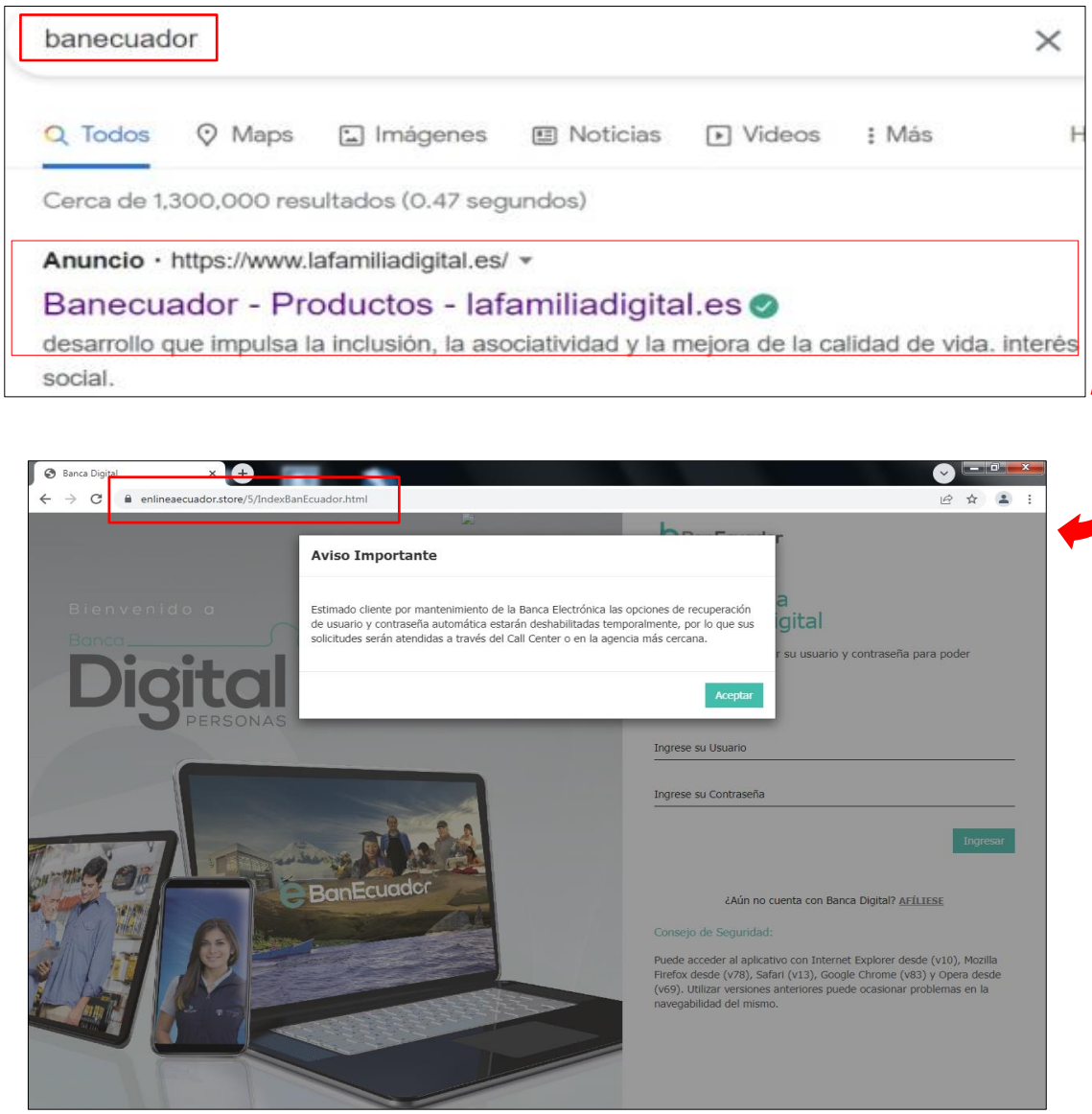

Figura 1.- ***Suplantación de identidad banca digital BANECUADOR***

Nro. Alerta:	EC-2022-42	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-feb-2022	**EcuCERT advierte nueva campaña de pharming en "BANECUADOR"**	V 1.1

VI. RECOMENDACIONES:

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

- Cuando se requiere acceder a un sitio web, ingrese el nombre de la empresa en el buscador y seleccione una opción de la página de resultados, observe detenidamente la redacción de los textos, los colores, la estructura o si existen cambios que puedan ser indicio de falsificación.
- 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; recuerde que un ataque de pharming puede venir acompañado de un primer ataque de phishing.
- Instalar y mantener actualizado una solución antivirus / antimalware
- Bloquear el sitio web indicado en la sección indicadores de compromisos
- Informarse continuamente sobre tipos de amenazas en la internet.
- 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.
- Borra la caché del navegador regularmente para eliminar los sitios web que pudiesen redirigirse a una copia fraudulenta.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec