Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

I. DATOS GENERALES

Clase de alerta: Phishing
Tipo de incidente: Suplantación de Identidad
Nivel de riesgo: Medio

II. ALERTA

En redes sociales circulan campañas de tipo maliciosas que toman la identidad de la Agencia Nacional de Tránsito (ANT) y la empresa TERPEL, la primera hace referencia a consultas de supuestas infracciones de tránsito en un sitio Web y la segunda a un portal de premios ofertados por la empresa. Las dos campañas están orientadas a obtener datos de tipo personal y se encuentran relacionadas. A continuación se presentan las capturas de los sitios:

Figura 1.- Campañas maliciosas a nombre de Agencia Nacional de Tránsito y TERPEL

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

III. INTRODUCCIÓN

La técnica de Phishing es una forma de fraude a través de medios digitales que pretende engañar a las víctimas para obtener información personal-confidencial tales como credenciales de cuentas de correo, banca electrónica, etc.

Este tipo de técnicas ha sido utilizado para suplantar la identidad de la Agencia Nacional de Tránsito (ANT) y la empresa TERPEL.

IV. VECTOR DE ATAQUE

Phishing

V. IMPACTO

A continuación se realiza el análisis de las dos campañas y su relacionamiento:

Agencia Nacional de Tránsito – ANT:

Los atacantes se sirven de publicaciones en redes sociales, suplantando la identidad de la Agencia Nacional de Tránsito, adjuntan un link de acceso a un portal Web de tipo malicioso (hxxps://sinta[.]sjk[.]co[.]id/[.]tmb/citaciones[-]ant/ANT[-]persona/), con el objetivo de extraer datos de tipo personal, así como también información de tarjetas de débito/crédito.

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 2.- Campaña maliciosa a nombre de Agencia Nacional de Tránsito

Como se evidencia en la Figura Nro. 2, los datos que solicita el sitio Web de tipo fraudulento, son: cédula de identidad, nombres completos y dirección de correo electrónico; posteriormente, al dar clic en el botón "Ingresar", el sitio Web de tipo malicioso direcciona a otra ventana a través de la que se alerta de una supuesta infracción de tránsito existente adicionalmente se solicitan datos de tarjeta de crédito/débito para realizar el pago de la misma (Figura Nro. 3).

Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 3.- Datos financieros que sustrae la campaña maliciosa a nombre de Agencia Nacional de Tránsito

Al dar clic en el botón "Pagar", el sitio Web alerta sobre un supuesto problema para realizar la transacción, solicitando otro método de pago, esta acción se realiza con el objetivo de hurtar la mayor cantidad de información bancaria (Figura Nro. 3).

TERPEL:

Durante la investigación del incidente de la Agencia Nacional de Tránsito, debido a una mala configuración del servidor de tipo malicioso (directorio expuesto), se pudo demostrar que en el mismo servidor en donde se aloja el sitio Web de suplantación de identidad de la Agencia, también se aloja un sitio Web de recolección de datos suplantando la identidad de la empresa distribuidora de productos derivados de petróleo y gas "TERPEL": hxxps://sinta[.]sjk[.]co[.]id/ganadores (Figura Nro. 5).

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

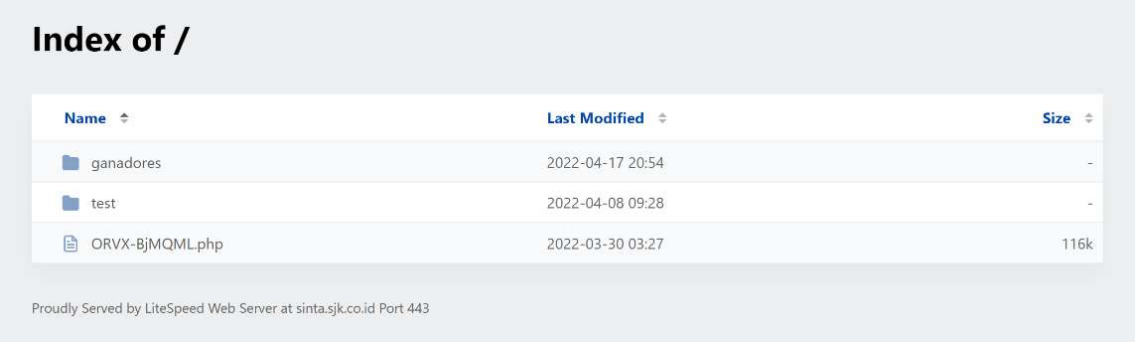

Figura 4.- Directorio de servidor Web que aloja campaña maliciosa a nombre de Agencia Nacional de Tránsito

Como se evidencia en la figura Nro. 4, en el servidor de tipo malicioso, existe un archivo llamado **ORVX-BjMQML.php,** el que, abre una ventana de login para un servicio de Shell Web que se muestra en la figura Nro. 5.

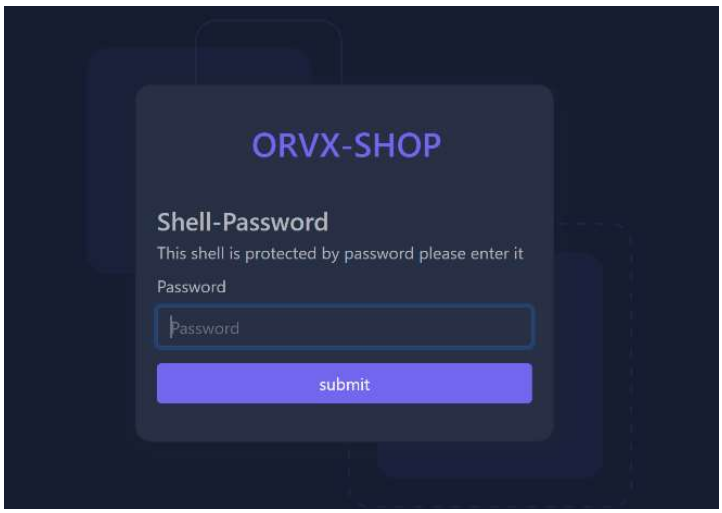

Figura 5.- Shell Web alojada en servidor de tipo malicioso

El servicio de la figura Nro. 5, hace referencia a un sitio Web de ciberdelincuentes, a través del que, se venden servicios de WebShell, CPanel y RDPs de algunos sitios Web/hosts alrededor del mundo. En la figura Nro 6. se observa información del sitio ORVX.

Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

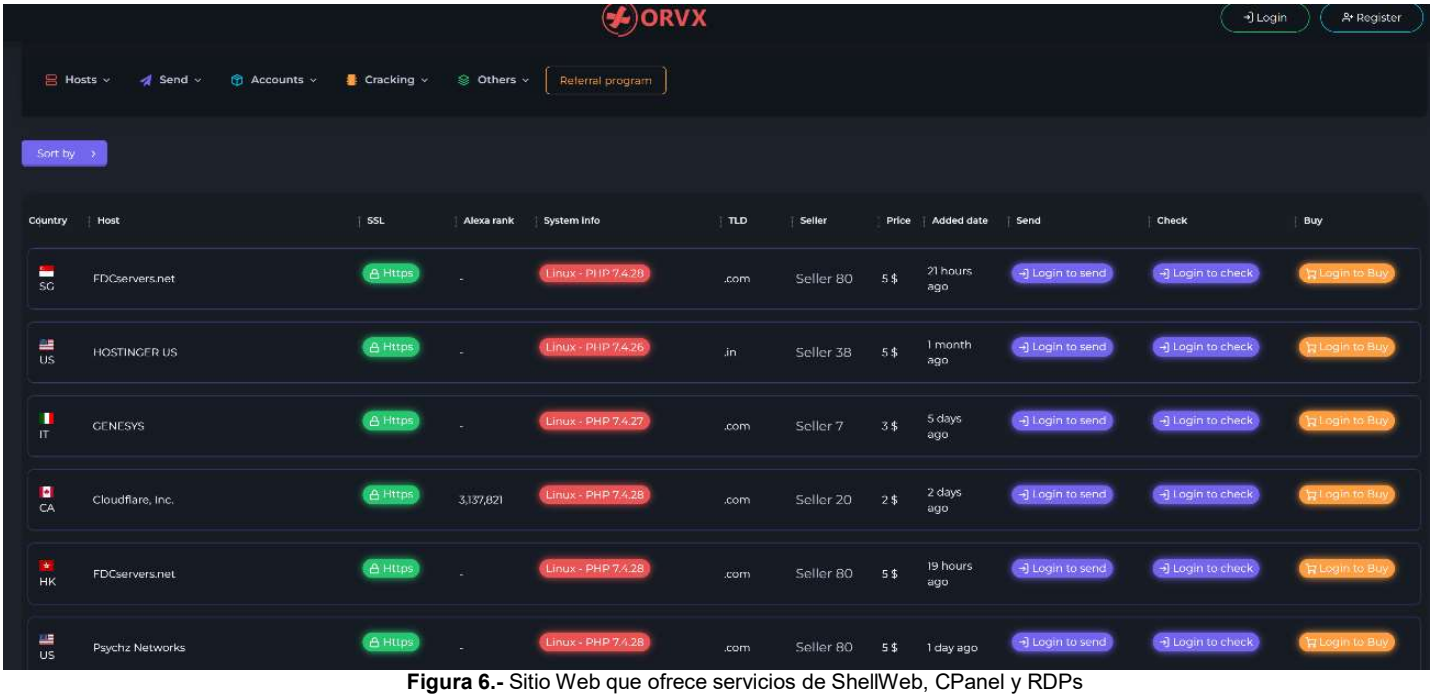

Figura 6.- Sitio Web que ofrece servicios de ShellWeb, CPanel y RDPs

Respecto a la Figura Nro. 7, (hxxps://sinta[.]sjk[.]co[.]id/ganadores/) se evidencia que el objetivo de la campaña de suplantación de identidad de TERPEL, sería de igual forma, hurtar información de tipo personal y bancaria, de una forma más sofisticada que la campaña de la Agencia Nacional de Tránsito, como se demuestra en la interacción con la campaña de acuerdo a las figuras Nros. 8, 9, 10, 11 y 12 mostradas a continuación.

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 7.- Campaña de tipo maliciosa de distribuidora de productos derivados de petróleo y gas "TERPEL"

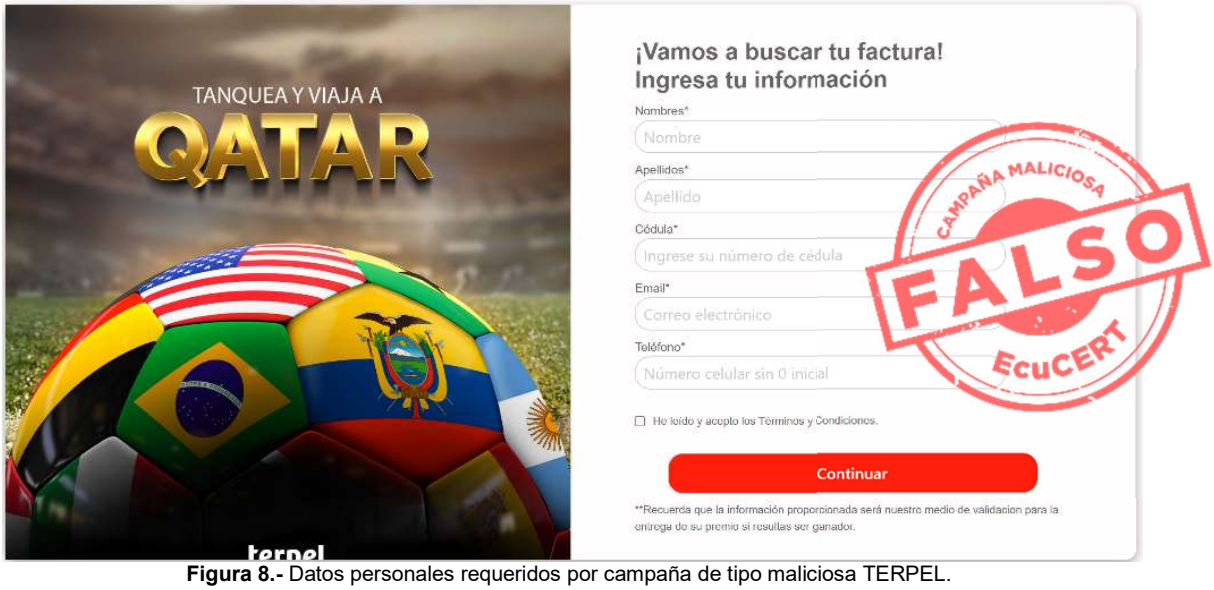

Figura 8.- Datos personales requeridos por campaña de tipo maliciosa TERPEL.

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 9.- Datos personales requeridos por campaña de tipo maliciosa TERPEL

Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 10.- Campaña de tipo maliciosa TERPEL

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

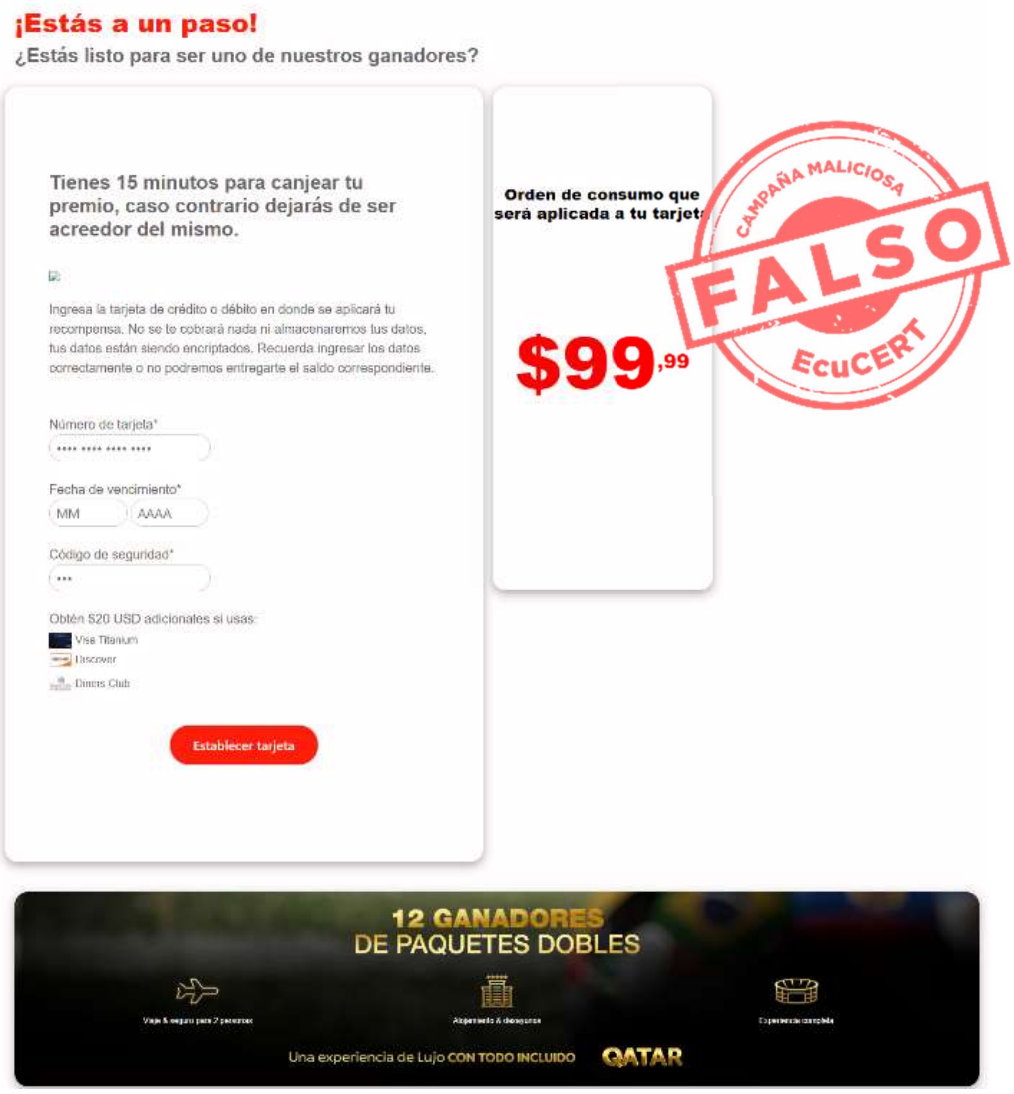

Figura 11- Datos personales requeridos por campaña de tipo maliciosa TERPEL

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 12.- Datos personales requeridos por campaña de tipo maliciosa TERPEL

Al analizar el código fuente de los sitios Web maliciosos, se evidencia que, todas las plantillas, así como también formatos, interfaz e interacciones, son extraídos de sitios Web lícitos en Ecuador: https://sites.placetopay.ec/ant/login, para el caso de la Agencia Nacional de Tránsito, y, https://terpelsicumple.com/ para el caso de la distribuidora de productos derivados de petróleo y gas "TERPEL". Que se muestran en las figuras Nros. 13 y 14 a continuación:

Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

Figura 13.- Sitio Web lícito de pagos ANT

Nro. Alerta:	EC-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

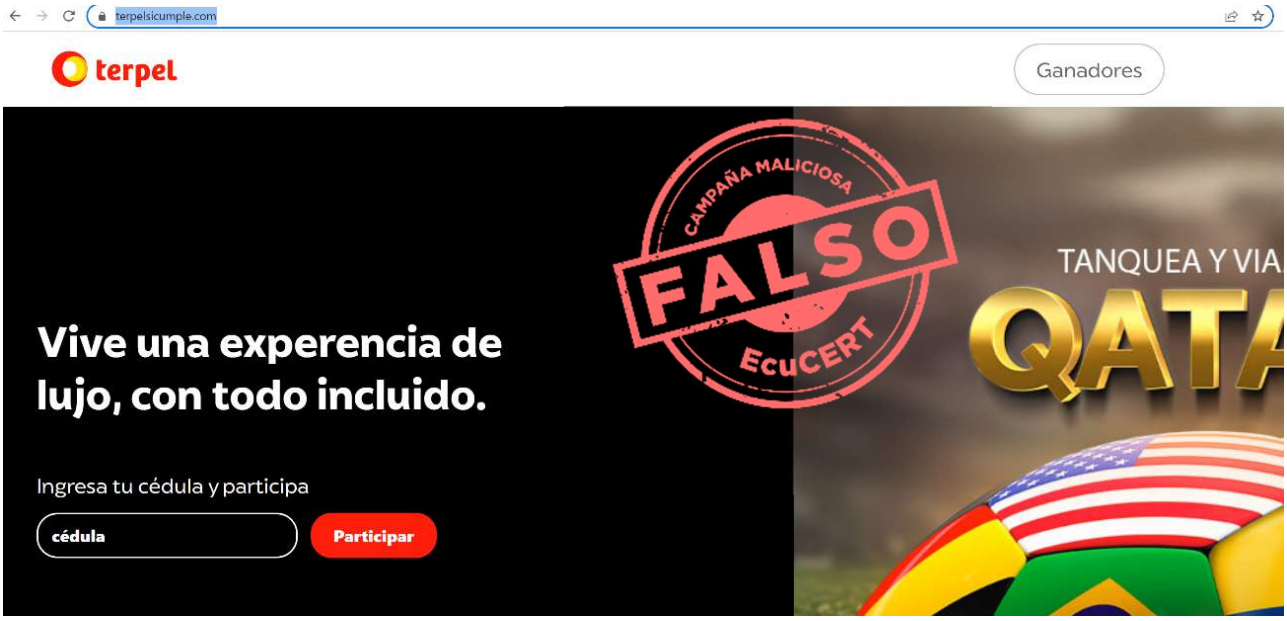

Figura 14.- Sitio Web lícito de promoción TERPEL

VI. INDICADORES DE COMPROMISO

Descripción	Valor
Dirección Web	https://rb[.]gy/qyqrx1
Cadena de Redirección	https://rb[.]gy/qyqrx1 https://sinta[.]sjk[.]co[.]id/.tmb/citaciones-ant/ANT-persona/ http://2m[.]ma/ https://2m[.]ma/ https://rb[.]gy/ar https://sinta[.]sjk[.]co[.]id/ganadores/ https://sinta[.]sjk[.]co[.]id/ganadores/loaders/cargando.php https://sinta[.]sjk[.]co[.]id/ganadores/factura.php

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-2022-62	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTA DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	21-abril-2022	**Suplantación de identidad "Agencia Nacional de Tránsito" y distribuidora "TERPEL"**	V 1.3

	https://sinta[.]sjk[.]co[.]id/ganadores/loaders/cargando2.php
Dirección IP de servicio	13[.]248[.]219[.]100
Link de Re direccionamiento para el pago	https://sinta.sjk.co.id/.tmb/citaciones-ant/ANT-persona/citacion.php https://sinta.sjk.co.id/ganadores/premio2.php

Tabla 1.- IOC asociados a campañas maliciosas.

VII. RECOMENDACIONES

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

- No abrir, manipular, o interactuar con correos electrónicos altamente sospechosos recibidos en las respectivas bandejas de correo electrónico ya sean personales o Institucionales.
- Prestar atención a los detalles de mensajes recibidos a través de redes sociales ya sean personales o Institucionales.
- Ante cualquier duda, contactarse directamente con la persona o empresa para su comprobación y/o denuncia.
- 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).
- Nunca entregue credenciales de usuarios, contraseñas, datos bancarios, o cualquier otro tipo de información de tipo personal, solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas, sitios web desconocidos.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa a nivel Nacional.

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