	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 073	**Fecha: 14-03-2022**
		Página 8 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de Alerta	Campaña de Smishing suplantando la identidad de "MegaPlaza y Corporación Toyota Motors".			
Tipo de Ataque	Suplantación		Abreviatura	Suplantación
Medio de Propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros			
Código de familia	G	Código de Subfamilia	G03	
Clasificación temática familia	Fraude			

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo diferentes delitos informáticos, empleando el denominado "Smishing", esta modalidad de estafa se realiza mediante mensajes de texto (SMS), a teléfonos móviles, utilizando como cebo haber ganado una camioneta cero kilómetros más S/50.000 mil soles**,** tomando el nombre de Percy Luis VIGIL VIDAL, representante del área legal de ***"PROMOCIONES DEL SORTEO MILLONARIO DE MEGAPLAZA Y CORPORACIÓN TOYOTA MOTORS",*** lo que hace más convincente a la víctima, para que accedan a un enlace que contiene el mensaje, con el objetivo completar formularios y revelar sus datos personales.
2. Proceso del ataque Smishing:

Imagen 01: Mensaje de texto enviado desde el teléfono 920266231 comunica lo siguiente: ***"Megaplaza le informa que su línea activa tiene un premio de S/50.000 + 1 Camioneta Hilux",*** debiendo ingresar en el enlace adjunto al mensaje.

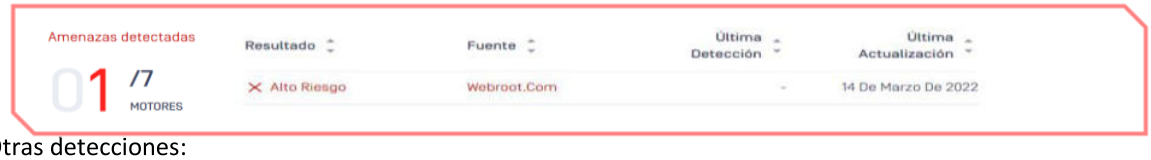
Imagen 02: Una vez hecho clic, en el enlace es redirigido a un sitio web falso que simula ser el oficial de "MegaPlaza", ofreciendo a la víctima, participar en un ***"SORTEO MILLONARIO DE MEGAPLAZA Y CORPORACIÓN TOYOTA MOTORS".***

Imagen 03: Luego, de unos segundos, aparece una ventana que requiere ingresar el DNI, para consultar si ha sido beneficiario de algún premio que ofrece el sorteo, lo cual deberá ***"VERIFICAR".***

Imagen 04: Finalmente, aparece lo siguiente: ***"FELICIDADES ERES AFORTUNADO GANADOR DE S/ 50.000 MIL SOLES Y UNA CAMIONETA PARA MÁS INFORMACIÓN LLAME A LOS NÚMEROS 971518326, 971620360 Y 934115904".***

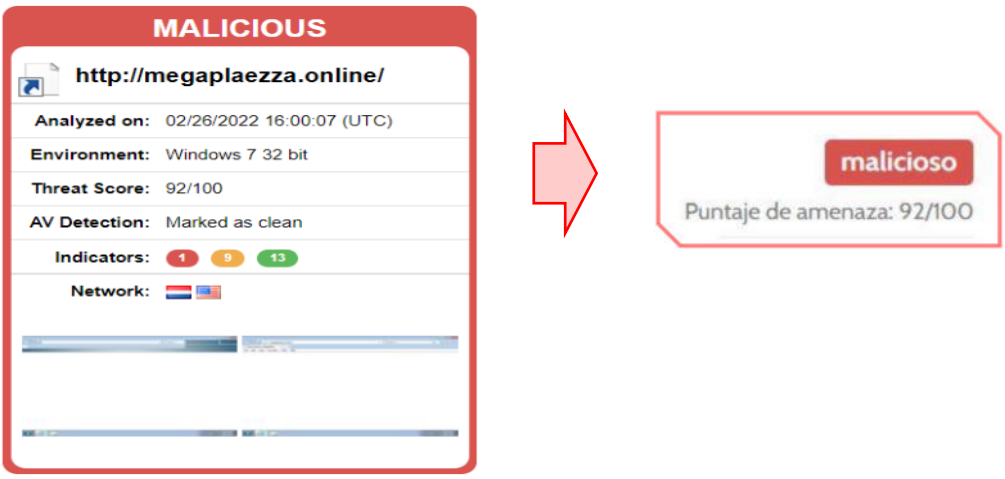
3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultado lo siguiente:

- Indicadores de compromiso:
  - URL: hXXp[:]//megaplaezza[.]online/
  - Dominio: megaplaezza[.]online
  - Dirección IP: 5[.]57[.]226[.]202
  - Código: 200
  - Longitud:880.18KB
  - SHA-256: 8ca4c692e0646f2c3e0d3f00667650e5bccfa305c7649fddfd89565d34d4d880



4. Otras detecciones:

- URL: hXXp[:]//megaplaezza[.]online/



5. Cómo funciona el Smishing:

- Los mensajes enviados a las víctimas, finge ser emitido por un banco, comercios u organismos gubernamentales alertando una situación de urgencia u oportunidad.
- Los mensajes contienen enlace que proporcionan más información o soluciones.
- Los mensajes vienen desde un número de celular de orígenes desconocidos o anónimos

6. Referencia:

- El Smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.), con el objetivo robar información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de teléfono o acceder a un enlace de una web falsa bajo un pretexto.

7. Recomendaciones:

- Evitar acceder a enlaces que forman aparte de un contenido de mensajes texto.
- Evitar proporcionar información confidencial por teléfono, WhatsApp, mensaje de texto, correo electrónico o redes sociales, a través de enlaces.
- Verificar la procedencia de los mensajes texto, en fuentes oficiales de la entidad que provee algún servicio o producto.
- Contar con una solución de seguridad, constantemente actualizada tanto en dispositivos de escritorio como en móviles, ya que sirven como barrera inicial protectora ante sitios web maliciosos.

Fuente de Información	Análisis propio de redes sociales y fuente abierta