	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 057	Fecha: 26-02-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Nueva campaña de Smishing que suplanta la identidad de "MegaPlaza y Consorcio Toyota Motors".			
Tipo de ataque	Suplantación		Abreviatura	Suplantación
Medios 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 informaticos empleando la modalidad de fraude "Smishing" que se difunde por medio de mensajes texto (SMS), a teléfonos móviles, donde los atacantes solicitan a las víctima, que visiten un sitio web que suplanta la identidad de "Mega Plaza y Consorcio Toyota Motors", utilizando como enganche haber ganado supuestamente una camioneta cero kilómetros más S/ 50.000 mil soles, con el objetivo completar un formulario y revelar sus datos personales.

2. Proceso del ataque Smishing:

Imagen 01: Mensaje de texto (SMS) enviado desde el número de teléfono +51 988 125 901 notifica sobre un supuesto premio ***"Felicidades! Eres un@ de nuestros ganadores de S/50.000 + 1 Camioneta, Gracias a Toyota y Megaplaza, Info: 971620360. Ing. Percy Vigil /"***, adjunto un enlace.

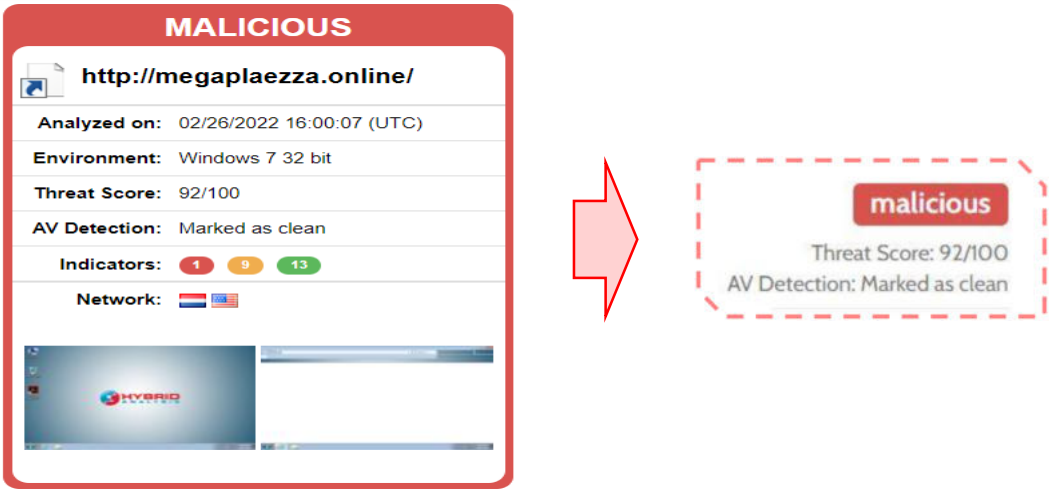
Imagen 02: Una vez hecho clic en el enlace adjunto al mensaje, es redirigido a un sitio web falso que simula ser el oficial de "MegaPlaza", donde hace referencia sobre un supuesto ***"SORTEO MILLONARIO DE MEGAPLAZA Y CORPORACIÓN TOYOTA MOTORS".***

Imagen 03: Luego, de unos segundos, aparece en la pantalla una ventana donde requiere que la víctima, ingrese su DNI, para consultar si ha ganado algunos de los premios que se ofrecen en el sorteo, deberá hacer clic en ***"VERIFICAR AHORA".***

Imagen 04: Finalmente, aparece una última ventana con el siguiente mensaje ***"FELICIDADES ERES 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
  - Tamaño: 880.18KB
  - SHA-256: 8ca4c692e0646f2c3e0d3f00667650e5bccfa305c7649fddfd89565d34d4d880



- Lista negra / IP: 5[.]57[.]226[.]202

4. 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.

5. 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.

6. 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.

Fuentes de información	Análisis propio de redes sociales y fuente abierta