Ciudad de México, a 1 de febrero de 2017

COMUNICADO DE PRENSA

CON *SOFTWARE* POLITÉCNICO DETECTAN ELEMENTOS MALICIOSOS EN IMÁGENES

- **El programa está basado en el funcionamiento del sistema inmunológico y distingue entre los elementos buenos y malos**
- **Diseñado para analizar fotografías de redes sociales**

C-066

Las redes sociales como *Facebook*, *Twitter*, *WhatsApp* y el correo electrónico son vías de comunicación utilizadas diariamente por millones de personas que comparten información e imágenes, las cuales en ocasiones contienen *software* malicioso, que dañan computadoras y dispositivos móviles.

Ante ello, los investigadores Moisés Salinas Rosales y Nareli Cruz Cortés, del Centro de Investigación en Computación (CIC) del Instituto Politécnico Nacional (IPN), desarrollaron un programa, basado en el sistema inmunológico, que identifica y elimina el *stegomalware*, elementos maliciosos ocultos en imágenes con formato JPG.

El núcleo del sistema politécnico funciona con un algoritmo bioinspirado en los sistemas inmunes artificiales, el cual, al igual que el humano distingue a las células buenas y malas dentro del organismo, así que reacciona ante la presencia de elementos extraños, de ese modo el *software* lo emula y analiza los componentes de las fotografías, explicó Salinas Rosales.

La innovación radica en que al estudiar un pequeño conjunto de elementos buenos, los algoritmos aprenden cuáles son las características que etiquetan a las fotografías portadoras de código malicioso. Tras analizarlas el programa detecta la amenaza y la elimina, así evita que se comparta el virus y propague por redes sociales.

Para comprobar la efectividad del *software* se utilizaron los métodos más novedosos de colocación de *stegomalware* (*F5*, *Outguess* y *Steghide*) en la inserción de contenido malicioso en mil 500 imágenes que posteriormente fueron analizadas.

Al hacer la evaluación se comprimen las fotografías y se extraen sus características para obtener una especie de huella digital, similar a un espectograma, donde se observan distintas frecuencias y gamas de colores. Cuando se presentan pigmentos muy contrastantes a su tonalidad, significa que existe un código malicioso oculto.

El sistema bioinspirado se entrenó con el análisis de 3 mil imágenes en calidad 720 HD, de las cuales 50 por ciento contenía *stegomalware*. Después se dio la instrucción para que cuando detecte elementos sospechosos alerte al usuario de que éstos se eliminen, agregó, la catedrática Nareli Cruz.

El *software* está creado con los lenguajes de programación *Python* y *C*, utilizados normalmente en temas de ciberseguridad. La meta inmediata es transformar el proyecto politécnico en una *app*, similar a un antivirus, para dispositivos electrónicos con sistema operativo *Android*.

El investigador politécnico recordó que ya existe el registro del *software* ante el Instituto Nacional del Derecho de Autor (*Indautor*) por parte del IPN, bajo el nombre

"Componente de análisis estenográfico para imágenes", el cual es el único que utiliza un sistema basado en algoritmos bioinspirados.

===000===

===000===