Ciudad de México, a 28 de febrero de 2017

COMUNICADO DE PRENSA

GARMDROID, SISTEMA POLITÉCNICO QUE DETECTA APPS CON MALWARE

- **Existen dos versiones, la página web y la aplicación para *Android***
- **Identifica las aplicaciones *hackeadas* provenientes de distintas tiendas**

C-158

Investigadores del Instituto Politécnico Nacional (IPN) desarrollaron *Garmdroid*, un servicio web y móvil que detecta las *apps* que contienen código malicioso. El sistema tiene 96.26 por ciento de efectividad y utiliza la tecnología *machine learning* para analizar los archivos en formato APK de las aplicaciones del sistema *Android*.

También muestra los resultados de manera amigable al usuario con ilustraciones y la lista de los componentes a los que la aplicación tiene acceso, como la cámara, el micrófono, la ubicación y los contactos, comentó Ponciano Jorge Escamilla Ambrosio, académico del Centro de Investigación en Computación (CIC).

Por norma general *Google* depura la *Play Store* para eliminar aquellas *apps* que incumplen sus reglas o suponen un riesgo para los dispositivos *Android* por contener *malware, "existen aplicaciones reempaquetadas o hackeadas que ocultan un código malicioso, bajo la apariencia de un programa de uso común, ya sea Facebook, WhatsApp o Youtube", detalló el profesor del CIC.*

Al ejecutar *Garmdroid* se muestran datos que identifican a la *app*, uno de ellos es el número de serie llamado SHA, que se genera de acuerdo con su contenido, por ello, si una ha sido reempaquetada con *malware*, el nombre será diferente al original.

Otra fuente de *apps* maliciosas son las tiendas y sitios web no oficiales, las cuales son identificadas cuando *Garmdroid* las escanea y muestra los permisos que solicitan para controlar el *smarthphone*. Por ejemplo, una aplicación que simula a una linterna no debe tener acceso a la cámara, micrófono o a la libreta de contactos.

Escamilla Ambrosio mencionó que la investigación se enfocó en los *smartphones Android* porque son los que dominan el mercado, y ahora prácticamente los celulares realizan operaciones que anteriormente sólo hacían las computadoras, como transacciones bancarias o usar las redes sociales.

La versión web trabaja con herramientas de *software* que están en un servidor, las cuales desempaquetan los archivos APK de la *app* y ejecutan un análisis estático, sin instalar el archivo en el equipo. Sin embargo, su complemento móvil examina todas las aplicaciones del celular, indica si son maliciosas o benignas y ofrece la opción para desinstalarlas.

El investigador del CIC explicó que se entrenó al clasificador de *Garmdroid* con *apps* benignas y maliciosas, con versiones modificadas y originales de diferentes tiendas. Para ello, utilizaron la base de datos del sitio *Virus Share* y de la *Technische Universität Braunschweig* de Alemania. El sistema politécnico analizó cinco mil aplicaciones para la versión móvil y más de 11 mil en el servicio web.

La aplicación creada con los lenguajes de programación *Python* y *Bash* está basada en las capacidades de desarrollo de *software* (SDK) de *Android*, especialmente por *Android Asset Packaking Tool*, con la finalidad de que el usuario sólo suba el archivo de la *app*, AndroidManifest.xml y realice el análisis vía web.

Se planea que la versión móvil de *Garmdroid* se libere en abril, mientras que la versión web ya está disponible gratuitamente en *http://www.garmdroid.org/*

En *Garmdroid* participaron además del CIC, las escuelas superiores de Cómputo (*Escom*), de Ingeniería Mecánica y Eléctrica (ESIME), ambas del IPN, y el Consejo Nacional de Ciencia y Tecnología (*Conacyt*).

===000===