INSTITUTO POLITÉCNICO NACIONAL
COMUNICADO DE PRENSA
COORDINACIÓN DE COMUNICACIÓN SOCIAL

México, D.F., a 05 de abril de 2015

COMBATEN ROBO DE INFORMACIÓN EN DISPOSITIVOS MÓVILES

- **Investigadores del CIC desarrollaron un proyecto de seguridad en cómputo para mitigar los efectos provocados por el *malware***
- **Los *hackers* extraen información sensible de dispositivos móviles por medio del software malicioso**

C-073

Con la finalidad de ayudar a los usuarios de dispositivos móviles que presentan incidentes de seguridad por códigos maliciosos como el *malware*, investigadores del Centro de Investigación en Computación (CIC) del Instituto Politécnico Nacional (IPN) trabajan en mitigar los efectos provocados por software malintencionado que se propagan en la red e incluso fuera de ésta.

“Este proyecto de seguridad en cómputo responde a la importancia de mitigar los efectos provocados por el *malware* a través de su análisis y modelado en dispositivos móviles, con la intención de aplicar los resultados en el diseño de controles robustos que prevengan el robo de información, a través del uso de algoritmos capaces de identificar comportamientos desconocidos llamados ataques del día cero”, indicó el doctor Eleazar Aguirre Anaya, titular del proyecto.

Desde hace algunos años, el procesamiento, almacenamiento y distribución de la información han estado vinculados con el avance de la tecnología.

Este avance ha permitido que la información esté disponible en todo momento y lugar. Los representantes más significativos son los dispositivos móviles, que permiten a los usuarios acceder a la información desde su hogar, trabajo, escuela y espacios públicos sin límites de conectividad y energía cambiando por completo sus hábitos.

Sus capacidades tecnológicas posibilitan el almacenamiento de fotografías, documentos de trabajo, correos, información de redes sociales, aplicaciones de todo tipo, entre otras, en un solo dispositivo, por lo que el individuo lo usa de manera indistinta tanto para su entretenimiento como para su trabajo.

“Los *hackers* han aprovechado todo lo anterior para extraer la información sensible almacenada en estos dispositivos por medio del software malicioso. Existen diversos controles de seguridad diseñados para mitigar la posibilidad de robo de información, sin embargo, las estadísticas indican lo contrario, día a día se incrementan los incidentes en sitios bancarios, compras electrónicas, pago de servicios e impuestos en línea, todos provocados por el uso de dispositivos móviles”, indicó el investigador politécnico.

Dijo que “un dispositivo móvil es el equivalente a tener un arma; si no la sabes utilizar, si no te haces responsable, puedes estar cometiendo algún delito aunque tú no lo sepas, ni tengas conocimiento que tal acción puede tener sus repercusiones”.

En el Laboratorio de Ciberseguridad del CIC se desarrolló la primera etapa del proyecto a través de un análisis de comportamiento del *malware*. Se tienen dos enfoques: el primero se aplica a cualquier tipo de red con comportamiento del *malware* y, el segundo, al análisis del *malware* en el sistema operativo, ambos a nivel de dispositivos móviles.

También se realizó una revisión a los dos estándares de procesos de manejo de incidentes más importantes en el mundo en cuestión de seguridad: la institución académica estadunidense SysAdmin Audit, Networking and Security Institute (SANS) y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).

El resultado fue que no se cubre satisfactoriamente el manejo de incidentes en móviles en ninguna de las mencionadas instancias.

El *malware* actualmente tiene comportamientos diferentes cuando se conecta en una red Wi-Fi o en una red celular. La red Wi-Fi tiene en su mayoría un conjunto de controles de seguridad más robustos, haciendo más factible la detección del *malware*, sin embargo, para el caso de la red celular, esto depende del proveedor de servicio y si ataca o no la infraestructura de comunicación.

Mientras el *malware* no ataque al consignatario del servicio, el proveedor no va a detener o limitar el ataque. Principalmente, el *malware* ataca al usuario final, es decir, a las personas con un dispositivo móvil, señaló el doctor Eleazar Aguirre Anaya.

===000===