Comunicado 110
Ciudad de México, 23 de abril de 2019

COMBATE IPN MALWARE CON LABORATORIO DE CIBERSEGURIDAD

- ***Ante el crecimiento de las amenazas informáticas, el Laboratorio de Ciberseguridad del Centro de Investigación en Computación (CIC) analiza el Malware para crear mecanismos de defensa***

- ***Empresas de seguridad internacionales detectan al mes aproximadamente 20 millones de muestras de software malicioso en el mundo***

El crecimiento de las amenazas informáticas plantean un nuevo paradigma de seguridad, por ello el Instituto Politécnico Nacional (IPN) se encuentra a la vanguardia en el análisis y detección de prácticas de Malware a nivel nacional, a través del Laboratorio de Ciberseguridad del Centro de Investigación en Computación (CIC), el cual aprovecha la vulnerabilidad de un sistema, la explota y crea nuevos mecanismos de defensa para fortalecer los niveles de seguridad cibernética.

El investigador del CIC, Raúl Acosta Bermejo, explicó que un Laboratorio de Malware es un espacio que cuenta con las herramientas necesarias para hacer análisis de este software malicioso. "En los últimos años, el concepto ha evolucionado, se mueve hacía una versión web o en la nube. El CIC tiene varios años trabajando en el estudio de Malware", acotó.

Detalló que este laboratorio ubica el Malware y lo analiza como si lo estudiara con un microscopio, ve su estructura, instrucciones y posteriormente se efectúan análisis estáticos. "Es un estudio sin tener que ejecutar; principalmente se revisa su código binario y además se realizan estudios dinámicos donde se corre el malware y se obtiene su comportamiento, es decir, se identifican sus actividades para modificar o borrar archivos", refirió.

"Por eso es importante que el laboratorio tenga todo lo necesario para verificar si el Malware está destinado a una Mac o Iphone. Entonces necesito un dispositivo para emularlo, pero si corre en una plataforma de Linux o en un servidor, es necesario introducir la muestra a una serie de aparatos para medir con sensores o herramientas y así saber lo que pasa", subrayó.

Acosta Bermejo enfatizó que en el laboratorio también detectan con quién se quiere comunicar el Malware, qué archivos lee, escribe, modifica y, en el caso del sistema operativo Windows, comprobar si cambia la configuración. "Este software malicioso sabe que hay programas que lo vigilan, como el antivirus y toma comportamientos evasivos, lo que se llama malware ofuscado, es decir, que se oculta", comentó.

"Lo más delicado, dijo, es que lo utilizan personas mal intencionadas para no personificarse y efectuar ataques en cualquier sistema computacional que tenga software y hardware. El Malware puede correr en los sistemas operativos más conocidos como Windows, Linux, Mac o Android y en casi todos los dispositivos móviles y tabletas, incluso en Blackberry".

Abundó que también se ha encontrado software espía en el Internet de las Cosas (IoT) como en los SmartWatch, en las cámaras web o en cualquier sistema donde se corra un programa. Existen áreas, indicó, que efectúan hackeos éticos; este laboratorio hace algo similar, toma una muestra del malware para analizarlo y crear nuevos mecanismos de defensa y de protección, así como nuevos algoritmos para antivirus.

"En la actualidad ocurren una gran cantidad de incidentes de seguridad relacionados con Malware. Las empresas de seguridad internacionales informaron que al mes se detectan aproximadamente 20 millones de muestras de Malware en el mundo. Esto quiere decir que se propaga mucho, por lo que falta hacer mucha concientización en las personas", afirmó el académico.

Finalmente, el investigador politécnico recomendó a los usuarios aplicar medidas para protegerse y que sus dispositivos no tengan daños. "Deben actualizar el sistema operativo, instalar un antimalware, tener buenas prácticas de uso de las aplicaciones, no instalar programas que no son oficiales o vienen de BlackStores (tiendas negras), así como mantener una salud física de los equipos de manera regular y revisar las herramientas instaladas, a efecto de que con estas acciones se reduzca la superficie de ataque", concluyó.

===000===