Ciudad de México, a 19 de mayo de 2017

COMUNICADO DE PRENSA

PRIMORDIAL CULTURA DE SEGURIDAD PARA EVITAR ATAQUES CIBERNÉTICOS: ESPECIALISTA DEL IPN

- **El primer filtro de defensa es el usuario entrenado**
- **Verificar las direcciones electrónicas, los *links* y los archivos para comprobar su seguridad**

C-392

El primer filtro de defensa ante un ataque cibernético debe ser un usuario bien entrenado que sepa distinguir los *emails* apócrifos y evite caer en el *phishing* al no abrir correos que contengan archivos con contenido malicioso (*ransomware*) o *links* que redireccionen a sitios sospechosos, comentó Moisés Salinas Rosales, especialista en seguridad de la información del Instituto Politécnico Nacional (IPN).

La defensa cibernética no sólo consiste en activar antivirus, *firewalls*, o medidas más complejas como Sistemas de Detección de Intrusión (IDS, por sus siglas en inglés) que monitorean constantemente el tráfico web de una computadora, que alertan cuando se visita un sitio extraño. También existe la opción de cifrar los discos duros o *software* de protección de redes. Para ello, es primordial un usuario bien entrenado y un equipo actualizado.

El investigador politécnico mencionó que abrir un *email* debe ser como cuando alguien toca a la puerta de tu casa, primero preguntas quién es y verificas si es confiable darle acceso. De lo contrario permites que se metan a tu computadora e instalen un archivo ejecutable o un DLL, oculto como un Word o PDF, que pone en riesgo tu equipo y el de los vecinos, lo cual puede desencadenar ataques cibernéticos como el ocurrido recientemente a nivel Mundial por el *ransomware WannaCry* o *WanaCrypt0r 2.0*.

Existe una mala cultura de la seguridad cibernética, se debe promover la importancia de verificar las direcciones electrónicas, los *links* de los *emails* y las extensiones de los archivos para comprobar su seguridad y autenticidad, para ello sólo basta con copiar el enlace y pegarlo en un block de notas para leer el nombre completo del emisor, dominio web y adjunto, recalcó el experto en ciberseguridad del Centro de Investigación en Computación (CIC).

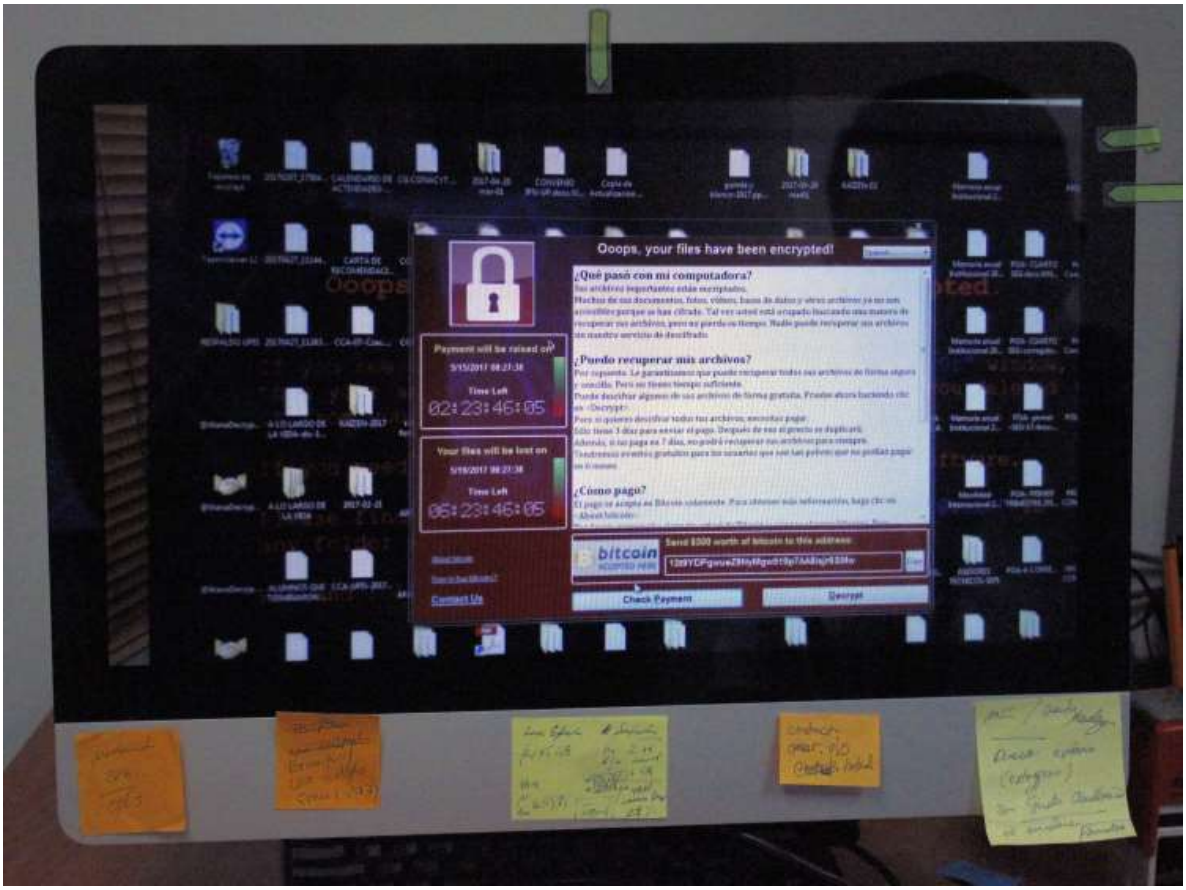
En el caso de *WannaCry*, el virus entró por vía *email*, el cual al abrir un archivo ejecutable, que pudo mantenerse oculto como un documento de Word o PDF, permitió la intrusión y el control del equipo. Después se cifró la información y generó una llave en la computadora infectada que mantuvo la información inservible. Al final se envió el *banner* que pedía rescate por el secuestro de los datos.

Algunas de las empresas afectadas por el *WannaCry* y que recibieron el aviso con instrucciones para efectuar el pago de bitcoins (moneda virtual) fueron Telefónica en Madrid, la automotriz Renault, así como varios hospitales del Servicio Nacional de Salud de Reino Unido e incluso al ministerio ruso.

Cuando un equipo se infecta con este virus la información se mantiene en la computadora, pero codificada, la cual sólo podrá ser restaurada con una llave que es tan compleja como un certificado o firma digital. Ante esto el experto del Politécnico recomendó, como parte de la cultura de la seguridad, el respaldo continuo de información, ya sea en disco duro externo o en la nube.

Por otra parte, comentó que el tema del *ransomware* no es nuevo, desde hace cinco años existen casos, sin embargo, este fue el primer ataque a gran escala en el que los puntos de inseguridad que dieron acceso al virus fueron los equipos deficientemente administrados y usuarios mal entrenados.

Muchos de estos ataques son del "día cero" porque explotan una debilidad que recién surgió, en este caso se aprovechó la vulnerabilidad del sistema operativo *Windows* que permitió el abuso de permisos y atributos por parte del intruso por medio de un puerto que ofrece un servicio específico, que sólo debería tener acceso a cierto contenido de tu equipo, pero esta vulnerabilidad propició que llegara al disco duro, tomara el control y que una vez dentro, el virus se propagara a través de equipos interconectados en diferentes redes, detalló Salinas Rosales.


Ooops, your files have been encrypted!
¿Qué pasó con mi computadora?
¿Puedo recuperar mis archivos?
¿Como pago?
Payment will be raised on
Time Left
02:23:46:05
Your files will be lost on
Time Left
06:23:46:05
bitcoin
Check Payment
Decrypt
Contact Us

===000===