La información, **nueva cara** de la guerra

AJ Singh, de la firma estadounidense de seguridad FireEye, conoce de cerca las actividades del grupo APT28, relacionado por algunos con el *hacking* gubernamental de élite y una de cuyas acciones más conocidas fue la infiltración de las últimas elecciones presidenciales en Estados Unidos. Revista Foros ISIS habló con él.

Hace unos años, cuando un vecino de AJ Singh supo que este pertenecía al FBI en Estados Unidos le dijo:

—Ah, entonces usted puede entrar a mi correo y leer mis mensajes.

—Sí, pero no tengo tiempo, pues ni siquiera alcanzo a leer los míos, le respondió Singh, quien trabajó 10 años para el Buró Federal de Investigaciones y ahora es director de Servicios Globales y Soluciones de Inteligencia de FireEye.

Con esta anécdota, el experto quiso mostrar cuán expuestos estamos a ser víctimas de ataques malintencionados en la web y cómo la información se ha convertido en una poderosa ciberherramienta de guerra de los Estados para alcanzar objetivos. Así ha ocurrido con los *hackers* APT28, los mismos que, en el 2016, *hackearon* los computadores del Partido Demócrata en Estados Unidos y robaron y divulgaron información, lo que pudo perjudicar a la candidata Hillary Clinton.

En su conversación con revista Foros ISIS, a propósito de su conferencia en el 4.º Foro en Seguridad de la Información, AJ Singh dio otros ejemplos de actividades maliciosas como la manipulación rusa de los resultados de las pruebas antidopaje en el Juegos Olímpicos de Sochi en el 2014, que fue denunciada por Wada (Agencia Mundial Antidopaje, por su sigla en inglés). "Encontramos el lanzamiento de documentos y correos de Wada por personas que trataban de ser activistas y vimos su relación con el APT28, pues se basaban en la infraestructura y las técnicas compartidas en comportamientos anteriores de esta amenaza", dijo.

La sigla APT se traduce como amenaza persistente avanzada, aunque el experto

Imagen: Pete Linforth (HypnoArt) en www.pixabay.com (https://goo.gl/CtQCbk). Licencia CCO Creative Commons.

Los ataques pueden provenir de activistas relacionados incluso con gobiernos, que envían mensajes propagandísticos para incidir en la geopolítica.

Foto: Felipe Cazares

AJ Singh, de FireEye.

La recomendación

Una clave para mejorar la seguridad de los ciudadanos es entender los riesgos, pues así es posible reducirlos.

"Es como en el fútbol. Si mis amigos y yo nos enfrentamos a una selección nacional, nuestro objetivo no es vencerla, sino perder por menos de 10 goles. Y cómo lo voy a hacer: debo entender cómo juegan para poder rendir mejor. Sé que voy a perder, pero por lo menos que no me ganen por tanto". dijo AJ. Singh.

aclaró que no necesariamente tiene que ser avanzada, pero la persistencia sí es una condición esencial. Añadió que en FireEye han detectado el surgimiento de activistas que envían mensajes propagandísticos, relacionados incluso con Estados como Rusia y precisó: "Aunque la información ha sido usada para fines similares desde la Guerra Fría, ahora es mucho más fácil y no cuesta tanto dinero. Lo único que se necesita es ir a un cibercafé de internet, tener conocimiento de cómo atacar un objetivo y causar algún daño. Depende de mis capacidades como autor y de tener acceso a un dispositivo".

Según él, es difícil establecer con certeza si los integrantes de APT28 son rusos o pertenecen al gobierno de ese país, pues a no ser que cada integrante cometiera un error operacional, habría que verificar la relación entre sus redes sociales y sus cuentas con algunas piezas de infraestructura que se hayan comprometido. "Lo que podemos decir es que sus actividades están alineadas con los intereses de los rusos, pero es difícil decirlo sin ver el teclado del *hacker*".

Ataques de Día Cero

Estas acciones malintencionadas contra aplicaciones o sistemas ocurren cuando las vulnerabilidades aún no han sido detectadas por los fabricantes o los usuarios y por lo tanto las fallas no han sido corregidas. Se consideran una de las principales armas de la guerra informática.

Por qué suceden. ¿Qué hace que los *hackers* malintencionados las detecten antes que las empresas o los gobiernos, que también tienen equipos de expertos avezados?

Para Aj Singh, la respuesta es financiera, en el sentido de que hay que evaluar los costos económicos, pero la buena noticia es que son ataques poco frecuentes porque requieren mucha investigación, tiempo y dedicación para poder encontrar las fallas en las aplicaciones. "Realmente, ahí es donde la ventaja radica en ser persistentes contra estas amenazas –aseguró–. Hay programas para encontrar esas vulnerabilidades y ponerles un parche, aunque otros estén trabajando para atacarnos".

Para Singh, la academia debe enseñar una programación responsable. "Es muy fácil entrar a Google, tomar un pedazo de código hecho por alguien, agregarlo a mi aplicación para que funcione y, aunque no sea a propósito, añadirle una vulnerabilidad. Así que es muy importante enseñarles a los estudiantes, a los amigos, a la familia, para que se defiendan y para que sepan cómo pueden ser unos expertos en el tema de la ciberseguridad", recalcó.

Otro problema es la escasez de talento preparado en ciberseguridad, pese a que es un trabajo muy bien pagado. "Hace un año di una conferencia en Savannah (Georgia, Estados Unidos). En ese Estado hay una comisión estudiando por qué hay 4000 plazas para seguridad, pero se gradúan menos de 15 con ese título y la mayoría regresa a sus países de origen. Hay un gran déficit no solo en tecnología, sino en personas y conocimiento".

Los antídotos de los **expertos**

Al final del foro se desarrolló un panel con los dos invitados internacionales y representantes nacionales. También hubo espacio para las preguntas del público. Revista Foros ISIS recoge parte de las intervenciones.

Cada panelista destacó una idea que quisiera que la gente recordara para mejorar su seguridad y privacidad cuando se conecta a internet. Coincidieron en que la educación de calidad y, sobre todo, innovadora es fundamental, para que no pase lo del cuento del pastorcito mentiroso: de tanto oír sus repeticiones, nadie le creyó.

Yenny Tatiana Rodríguez

La gestión del riesgo es fundamental. Todo tiene cosas buenas y malas y sea que creamos en nuevas ideas o en las tradicionales, es importante que sepamos a qué nos enfrentamos midiendo ese riesgo.

Martha Liliana Sánchez

No podemos dejarle la seguridad ciudadana solo al Estado; cada uno de nosotros es responsable y debe balancear los riesgos de seguridad y privacidad. Para obtener algo, siempre tenemos que arriesgar algo y la tecnología no es diferente.

Coronel Fredy Bautista

Cualquier dato en internet tiene un precio y eso cambia el paradigma de que solo se ataca a las grandes corporaciones y no al ciudadano de a pie. Por ejemplo, si a usted le toman una fotografía cuando está interactuando con el computador, pueden venderla para crear un falso perfil y generar una cadena de fraude y de cibercrimen.