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.

La seguridad es un asunto de todos. No podemos dejarla en manos del Estado, de unas pocas instituciones o de otras personas.

Eddy Williems

Crea en usted y en nadie más. Usted, como humano, es el factor crítico; está decidiendo y es responsable de lo que hace o de lo que va a suceder. Si hace la elección correcta, ganamos todos.

AJ Singh

Más bien le diría que sea consciente de que usted puede equivocarse, porque hay factores que no dependen de nosotros, sino de proveedores como los de servicios en la nube. Recuerdo un caso de un programa para limpiar el computador, que provenía de un proveedor confiable, era una herramienta legítima, pero la habían vulnerado.

Preguntas del público

¿Cómo podemos usar la inteligencia artificial al servicio de la ciberdefensa? ¿Ya lo estamos haciendo?

Martha Liliana Sánchez

En Colombia ya contamos con sistemas de detección temprana, proactivos, que pueden detectar indicios de un ataque cibernético y responder con ciertas reglas para prevenir ataques a infraestructuras críticas, aunque no están totalmente terminados.

También tenemos simuladores de guerra cibernética, que crean escenarios, toman decisiones y nos entrenan para actuar o para prevenir los ataques.

¿La seguridad que ofrecen las plataformas en la nube para almacenamiento de información puede ser suficiente para una pyme?

Eddy Williems

Cloud tiene muchísimas cosas buenas, pero hay aspectos para considerar como la confianza en el proveedor, pues así como uno se autentica en la nube para subir o bajar datos, también podría haber *malware* que se está haciendo pasar por uno.

En un país con tanta gente mayor, que no está familiarizada con internet, ¿cómo hacemos para hacerles llegar el mensaje de la seguridad?

Eddy Williems

Tanto en Estados Unidos como en Europa tenemos programas para niños pequeños y para adultos mayores, pero no es suficiente. Es muy difícil llegarles a las personas de 67 o 70 años y por eso he decidido ayudar a educarlos. Esta es una invitación para que todos colaboremos y no esperemos a que otros lo hagan porque esa es una posición muy cómoda, pero no siempre da buen resultado.

Martha Liliana Sánchez

La parte más débil de la cadena son las personas y la seguridad no se reduce a internet. He conocido casos de gente mayor que entrega los datos de sus tarjetas por teléfono, porque cree que si tiene el plástico en el bolsillo no podrá ser objeto de fraude. Una estrategia del Gobierno es educar a los niños desde el colegio y también a los profesores, muchos de los cuales no fueron nativos digitales. También hacemos campañas de comunicación estratégica con el Ministerio de Educación, la Presidencia de la República, Asobancaria y la Policía para sembrar en la gente la espinita de si será verdad o no lo que le están diciendo cuando la llaman por teléfono.

Coronel Fredy Bautista

Hemos trabajado el tema de la economía digital con la Cámara Colombiana de Comercio Electrónico y con Asobancaria y una de las conclusiones es que se necesita educación de calidad y concientización en todos los niveles, sobre todo para el usuario. El ciudadano común puede ser atracado cuando, por ejemplo, descarga una aplicación para ciclistas y publica la ruta que seguirá cuando salga a montar. Eso nos obliga a cambiar la conducta, a unirnos a grupos y a tomar las mismas precauciones que con las redes sociales, pues estamos vinculando algunos datos como el correo electrónico. A la par que hay nativos digitales, un grueso de población, entre la que me incluyo, se topó con la evolución y no podemos perder de vista que cada vez que damos un pestañazo encontramos una nueva modalidad de crimen.