laSegunda

Fecha: 22/10/2024 Audiencia: 33.709 Sección: ENTREVISTAS
Vpe: $1.517.446 Tirada: 11.692 Frecuencia: DIARIO
Vpe pág: $1.776.800 Difusión: 11.692
Vpe portada: $1.776.800 Ocupación: 85,4%

Dmitry Bestuzhev, experto ruso en ciberseguridad:

"La información financiera debería estar abierta a cualquier investigación criminal"

Por Paulina Modiano

"La ruta del dinero no está limitada al narcotráfico sino también a los ataques cibernéticos", dice el especialista que estuvo hace unos días en Chile participando en un seminario sobre cibercrímenes organizado por la PDI.

Uno de los lados oscuros del avance tecnológico está vinculado a las nuevas modalidades delictuales; hoy los llamados «cibercrímenes» están presentes en prácticamente todos los países.

Esta preocupante realidad fue abordada por el especialista ruso Dmitry Bestuzhev, en la séptima versión del seminario sobre ciberseguridad organizado —hace un par de semanas— por la Policía de Investigaciones (PDI) y la Universidad Federico Santa María (UFSM).

La presentación de Bestuzhev se tituló «Hackers de Elite: la infiltración de la Oficina 121 en América Latina», y apuntaba a perfilar la misteriosa organización ligada al gobierno de Corea del Norte, cuyo objetivo es atacar a las instituciones financieras para obtener dinero, aunque no se descarta que también intenten conseguir información clasificada de quienes considera enemigos.

"Ellos han estado presentes acá en Chile desde hace algunos años. Nosotros reportamos un primer ataque al Banco de Chile", cuenta Bestuzhev, quien ha estudiado en profundidad este caso apoyándose en sus más de 20 años de experiencia en seguridad informática: fue jefe de investigación y análisis global para Latinoamérica de la compañía rusa Kaspersky, y luego fue director del área de inteligencia contra ciberamenazas en BlackBerry. Su gran conocimiento de la realidad regional lo llevan a hacer un diagnóstico del país que, por decir lo menos, resulta inquietante.

"Chile es un país demasiado interesante para los atacantes porque tiene una conectividad muy grande. También es una economía que, a pesar de las críticas que puedan existir, es bastante estable y también con una concentración importante de negocios extranjeros. Todo esto crea condiciones que despiertan el interés de los atacantes internacionales", señala.

"Se hace difícil saber quién está detrás de toda operación"

—¿Cómo operan estos hackers de elite y cuáles son sus blancos principales?

—La «Oficina o Bureau 121» es una entidad que forma parte de la Agencia de Inteligencia del Estado norcoreano y su objetivo, por una parte, es causar daño a sus enemigos, pero principalmente generar ingresos para el gobierno. La razón es que Corea del Norte ha vivido muchísi-

laSegunda
Fecha: 22/10/2024 Audiencia: 33.709 Sección: ENTREVISTAS
Vpe: $1.531.668 Tirada: 11.692 Frecuencia: DIARIO
Vpe pág: $1.776.800 Difusión: 11.692
Vpe portada: $1.776.800 Ocupación: 86,2%

mos años bajo las sanciones internacionales y eso limita su acceso a divisas. Estas organizaciones operan de una manera compleja y estratificada, que determina quién es el responsable de cada cosa. A la cabeza están los especialistas en informática que diseñan los mecanismos tecnológicos para generar los ataques, quienes habitualmente se instalan en otros países con identidades falsas. Bajo ellos hay otros personajes que actúan como operadores intermediarios, o "mulas". Actualmente es el sistema de funcionamiento más habitual para realizar los delitos, porque los atacantes individuales casi no existen. Y eso se traduce en que se hace muy difícil saber quién está detrás de toda la operación y también saber a dónde va a parar el dinero.

—¿Es Corea del Norte el único país que se ha logrado identificar como operador de delitos cibernéticos?

—Cuando se trata de ataques a las instituciones financieras estamos hablando principalmente de Corea del Norte. Pero hay otros países que también tienen esas capacidades, por ejemplo, los pertenecientes a la antigua Unión Soviética como Rusia.

—Existen los ataques a grandes compañías, pero en Chile también se ha masificado la estafa a personas que reciben ofrecimientos de créditos a través de internet.

—Efectivamente estamos viendo otra modalidad orientada al ofrecimiento de préstamos a través de las plataformas digitales y ahí hay algo interesante, porque los recursos que están atrás también son grises y probablemente se trata de lavado de dinero. El esquema funciona en base a que una persona instala una aplicación para solicitar un crédito, y básicamente entrega toda la información de su vida en tiempo real, sus datos personales, el lugar donde vive, su familia, lo que da pie para que luego se produzca una intimidación y una extorsión. Entonces la víctima se siente completamente abandonada y acorralada.

—¿Estas son bandas organizadas?

—Sí, definitivamente. Incluso se invierte en publicidad para promocionar estos fraudes y los números muestran que esto ha crecido. Cuando se trata de ataques a las personas, ya sea por ofrecimiento de créditos o a clientes de bancos, generalmente su origen es Brasil, que tiene una verdadera casa productora de sistemas especialmente diseñados para atacar a personas.

"No se puede decir que Chile está del todo preparado"

—Usted señaló que Chile es particularmente atractivo para los delitos cibernéticos. ¿Cuán preparado cree que está el país para afrontarlos?

—La verdad es que no se puede decir que esté del todo preparado. Y no necesariamente porque esté muy atrasado en esta materia, porque estos criminales han atacado países europeos, de Asia o Estados Unidos. Realmente tienen la capacidad para hacer daño en cualquier parte y Chile, en este caso, no es una excepción. Aunque existen esfuerzos bien orientados, no son lo suficientemente efectivos para detener los ataques en las fases iniciales. Más bien vemos que sucede el ataque, comienza la investigación y el asunto aparece en la prensa; ese es el proceso.

> Chile es un país demasiado interesante para los atacantes cibernéticos porque tiene una conectividad muy grande".

> (Los hackers norcoreanos) han estado presentes acá en Chile desde hace algunos años. Nosotros reportamos un primer ataque al Banco de Chile".

—Eso quiere decir que no hay una capacidad de prevención frente a los ataques.

—No, en este momento no. Puede haber problemas por falta de herramientas, de recursos humanos, de competencia, pero lo que realmente debe existir es una gran coordinación si queremos trabajar por el bien de toda la sociedad. Si eso no ocurre, se crea una situación favorable, una especie de período de gracia para que los atacantes puedan operar. Por otro lado, para poder defender una infraestructura en un país, se necesita hacer ejercicios para saber si uno está realmente protegido y a qué nivel. Es un poco imitar el actuar del atacante para ver si mis sistemas están diseñados para resguardarme y si tengo la capacidad científica para detener el ataque.

—¿Cómo se puede lograr eso? En el caso de las compañías, éstas probablemente cuentan con recursos para disponer de equipos especializados que puedan realizar esa labor. Pero en el caso de los ciudadanos eso no ocurre, entre otras cosas porque muchas veces poseen conocimientos muy básicos en materia tecnológica.

—En algunos países ha habido un mayor éxito que en otros. Un caso es Israel, pero eso tiene que ver con la disposición de la gente, porque si ellos sienten que están bajo ataque tienen una mayor conciencia y una determinación de acatar las normas que se imponen. Pero en otros lugares en que no existe esa situación, está la posibilidad de que dentro de un círculo familiar o de confianza haya algunas personas más interiorizadas con el uso de la tecnología que pueda ayudar a otros que saben menos. También hay un tema cultural de por medio. En general, en Latinoamérica las personas son más abiertas, les gusta conversar, confiar, pero esa característica humana tan positiva, al mismo tiempo se puede convertir en algo que favorece a los atacantes, porque les resulta más fácil engañar a alguien. Lo importante es seguir implementado las mejores prácticas con las tecnologías, para saber cómo reaccionar y cómo mitigar esos ataques.

—¿Y cabe alguna responsabilidad a las empresas tecnológicas, en el sentido de no sólo vender sus servicios, sino de garantizar que sean lo suficientemente seguros frente a ciberataques?

—Ese es un tema complejo, porque si no existe una normativa que obligue a las empresas a proveer a los clientes de información que les permita no ser víctimas de ciberataques, es muy difícil que lo hagan voluntariamente, porque puede tener un impacto en sus costos. No se puede actuar sólo sobre la base de la buena voluntad, porque las empresas pueden decir que hacen campañas de capacitación, pero claramente eso no es suficiente. Tal vez se deba establecer algún sistema de incentivos, como crear un ranking de excelencia que muestre de forma certificada la cantidad de incidentes, no sólo a nivel local, sino también regional, que una compañía ha debido enfrentar. Eso es un beneficio reputacional para las empresas que les puede favorecer a conseguir más clientes.

—Chile está enfrentando actualmente un problema bastante severo de seguridad que ha tenido un fuerte impacto sobre la población, en especial por sus niveles de frecuencia y violencia. ¿Cree usted que se están haciendo esfuerzos significativos para abordarlo?

—Pienso que sí se está avanzando en comparación a otros países. En el caso de los ataques cibernéticos, lo que vemos es que están aumentado al igual que las víctimas. Entonces se requiere descubrir qué es los que está fallando, si es el discurso, las tecnologías o a la falta de educación.

—A su juicio, ¿cuál es la estrategia más adecuada para abordar la ciberdelincuencia?

—Bueno, básicamente seguir trabajando en distintos flancos: educación personal y corporativa; mejores tecnologías; leyes que realmente puedan funcionar y que no queden solamente en el papel. Cosas que estén orientadas a atacar el problema por todos lados e ir tratando de cerrar las brechas. Es una coordinación completa y hay que tener una medición en tiempo real de dónde estamos avanzando y dónde estamos fallando. Eso debe ser una práctica permanente.

—Si es así, aunque se requiera de esquemas coordinados entre distintos estamentos, públicos y privados, ¿la responsabilidad de esta tarea debe ser ejercida necesariamente por los gobiernos?

—Cuando se trata de defender a un país y la estabilidad de su economía, por supuesto que la responsabilidad tiene que ser del Estado. Se necesita de decisiones que vengan de arriba hacia abajo y no al revés.

—Pero ello requiere de una voluntad política. En Chile se están tramitando actualmente varias leyes en materia de seguridad, pero hay algunas que han tenido fuerte resistencia como el levantamiento del secreto bancario, lo que impide seguir la ruta del dinero y llegar a los cabecillas de bandas de narcotraficantes o cibercriminales.

—Ese es un problema real y son situaciones que no deberían existir, porque la ruta del dinero no está limitada al narcotráfico sino también a los ataques cibernéticos. El acceso a la información financiera no se debe cerrar, debería estar abierto a cualquier tipo de investigación criminal.