«Ransomware», el ciberataque que tiene en alerta a América

El «ransomware», una modalidad criminal con la que se secuestra información de una compañía, Gobierno o usuario para cobrar un rescate, tiene en alerta al continente americano, ante una ola de ataques que ha puesto a prueba sus relativamente inmaduros sistemas de ciberseguridad.

Luego de la crisis de 2021 en Estados Unidos por los ciberataques que afectaron a más de mil empresas y que llevaron al Gobierno a convocar una cumbre internacional para tomar medidas, el «ransomware» tiene ahora parpadeando en rojo a los sistemas de Latinoamérica, región que en los últimos meses ha afrontado una serie de irrupciones de alto impacto en lugares como Brasil, Perú y Costa Rica, país este último donde incluso se declaró emergencia nacional.

«El 'ransomware' triplicó su rentabilidad durante la pandemia y, aunque la esencia técnica sigue siendo la misma, su modelo de operación ha evolucionado drásticamente hasta convertirse en grandes y sofisticadas organizaciones criminales», explica a Efe Kerry-Ann Barrett, directora del Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA).

Un lucrativo y peligroso negocio

El «ransomware» se vale de un programa malicioso que impide a los usuarios entrar a su sistema o a sus archivos y exige el pago de un rescate para poder acceder a ellos nuevamente.

Aunque gran parte de las organizaciones no reportan estas extorsiones, la plataforma Ransomwhere, que rastrea desde hace un año los rescates, calcula que solo los pagos a los criminales en criptomoneda superan ya los 120 millones de dólares, de los cuales casi 17 millones se han entregado en 2022.

Para Marc Rivero, investigador del gigante ruso de ciberseguridad Kaspersky, esto explica el «gran avance de ese delito, puesto que que puede mover más dinero que la trata de personas o la venta de armas».

El Informe de Amenazas Cibernéticas 2022 de la firma estadounidense SonicWall, evidencia un repunte del 105 % en el secuestro de datos el año pasado, al superar los 623 millones de ataques en todo el mundo -casi veinte intentos por segundo-, con Estados Unidos a la cabeza (421 millones o el 67,5 % del total).

Del lado latinoamericano, Brasil (33 millones de ataques y cuarto en el mundo), Colombia (11,3 millones, sexto) y México (7 millone, décimo) se ubican entre los diez países más afectados por esa modalidad extorsiva, en una lista en la que aparece también Canadá, que ocupa el quinto puesto, con 24,2 millones de atentados.

El hecho de que Brasil sea el principal país latinoamericano atacado por este tipo de programas se atribuye a su mayor disponibilidad de servicios por internet, una situación que se disparó por las restricciones que impuso la pandemia.

En tanto, en México, el crecimiento en el último de año fue de cerca del 700 % en intentos de ciberataques a empresas y de hasta 1.000 % en dependencias del Gobierno, detalla Jesús García, gerente para México de Quest Software.

Y, en el caso de Chile, el Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Gobierno menciona que los intentos de ciberataque contra instituciones el pasado mes de abril rondaron el medio millón y buscaban la vulnerabilidad en sitios y sistemas web para robar la información del Estado y sus ciudadanos.

Sin embargo, «es muy difícil saber cuántos ataques de ransomware hay en Chile, ya que no siempre las instituciones o empresas afectadas revelan que han sido vulneradas. Y menos se conocen aún los casos que sufren las personas», informan en este organismo a Efe.

Una «guerra» en una región vulnerable

«Estamos en guerra y esa no es una exageración», declaró el mandatario de Costa Rica, Rodrigo Chaves, el pasado 16 de mayo, apenas ocho días después de asumir la Presidencia, refiriéndose al grupo de origen ruso Conti, autor de una serie de ataques tipo «ransomware» contra una treintena de entidades estatales.

Ese mismo grupo aseguró a comienzos de mayo que había atacado correos de la Dirección General de Inteligencia del Ministerio del Interior de Perú y reveló el seguimiento a funcionarios públicos y actividades virtuales de distintos ministerios.

Para los expertos, estas experiencias muestran que los delincuentes se están volcando en una región que consideran potencialmente rentable y con defensas de ciberseguridad relativamente inmaduras.

«Como Estados Unidos y Europa han aumentado su protección,

resulta un poco más sencillo para un ciberdelincuente buscar mercados o lugares en los que el nivel de protección es inferior», describe a Efe Belisario Contreras, quien lideró durante más de una década el Programa de Ciberseguridad en la OEA y ha sido copresidente del Consejo Global para el Futuro de la Ciberseguridad del Foro Económico Mundial.

«A Costa Rica le tocó esta vez, pero pudo haber sido cualquier otra institución de cualquier otro país de América Latina y el Caribe. A la región le hace falta un nivel más alto de madurez en ciberseguridad», añade Contreras, actual director sénior de estrategia global de seguridad y tecnología del bufete Venable LLP.

Como muestra de esa fragilidad, días atrás la Asociación de Bancos del Perú advirtió al Gobierno de una «brecha de seguridad» en los organismos del Estado que dejaba en riesgo los datos personales de ciudadanos en las redes sociales.

Mientras tanto, en México, señala Quest Software, el Gobierno ha aumentado el uso de código abierto (software cuyo código fuente está a disposición de todo el mundo), lo que representa otro motivo de vulnerabilidad.

Blancos y objetivos

De acuerdo con Barrett, todas las instituciones están en riesgo dado el grado de sofisticación de las estructuras «ransomware-as-service (RAAS)», que son «grupos de 30 a 60 personas con departamentos de recursos humanos, mercadeo, negociadores y desarrolladores, que se dedican las 24 horas del día a estudiar posibles objetivos y planificar ataques».

Y aunque en sus recientes irrupciones en Perú, el grupo Conti ha asegurado que trabaja «exclusivamente» por dinero, según la directora del Programa de Ciberseguridad de la OEA, hay también un interés mediático de «divulgar información confidencial o interrumpir o paralizar servicios» masivamente.

En el caso de América, los expertos de SonicWall y de Kaspersky han detectado que los ataques recientes de alto perfil han apuntado a empresas estratégicas de energía o consumo, Gobiernos, instituciones de educación y hospitales.

En esta línea, Estados Unidos fue blanco el año pasado de varios ciberchantajes a importantes infraestructuras y empresas, como Colonial, la mayor red de oleoductos del país, y JBS, principal procesador de carne del mundo.

Otro ataque de gran repercusión en la región comprometió al sistema de notificación del Programa de Inmunizaciones del Ministerio de Salud de Brasil a finales de 2021, en pleno pico de una nueva ola de la pandemia, y fue asumido por el grupo Lapsus con el mensaje: «contáctenos si quieren recuperar los datos».

La andanada también ha afectado durante el último año a una docena de entidades públicas de Colombia, el más grave de estos ataques fue contra el Departamento Administrativo Nacional de Estadística (DANE) y dejó fuera del aire su página web durante casi diez días, aunque gran parte de la información vulnerada se logró restablecer por los «backup» (respaldos) que mantenía la entidad.

También en Ecuador -país que según Kaspersky, es uno de los principales objetivos de los cibercriminales en Latinoamérica, junto con Brasil, México, Perú y Colombia- varias empresas y grandes instituciones han sido atacadas en los últimos meses, entre ellas la Agencia Nacional de Tránsito, la Corporación Nacional de Telecomunicaciones, el Banco Pichincha -el más grande del país- y el Municipio de Quito.

Respaldos y segmentación de la información

Tras la emergencia en Costa Rica y al cumplirse un año del caso de Colonial Pipeline, considerado el mayor ciberataque exitoso a la infraestructura petrolera en la historia de EE.UU., los expertos insisten en que hay que tomar medidas preventivas.

A este respecto, se considera clave segmentar los sistemas informáticos, para aislar los distintos componentes en caso de que se produzca un ciberataque.

«Otro factor muy importante son los respaldos, los «backup» que posibilitan volver en línea inmediatamente. Una solución para ello está en la nube, que permite tener respaldos descentralizados», subraya Belisario Contreras.

Mientras que Kerry-Ann Barrett, de la OEA, sugiere que como el 81 % de los ataques exitosos utilizan correos electrónicos como vectores, se implementen modelos de doble autenticación en las cuentas personales y corporativas.

EFE