TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLOGICO DE TIJUANA

SEMESTRE 2022-1

ING INFORMATICA

TALLER DE LEGISLACION INFORMATICA

ACTIVIDAD 1 UNIDAD 6

Garcia Vázquez Wesly

Docente: DANIELA ADRIANA SANCHEZ VIZCARRA

Lazarus, los cibercriminales que roban y extorsionan para el Amado Líder de Corea del Norte

El grupo de 'hackers' que en 2017 secuestró ordenadores de todo el mundo con el virus WannaCry acaba de robar 625 millones de dólares en criptomonedas, el mayor golpe digital de la historia

El mes pasado se perpetró el mayor robo cibernético del que se tiene constancia. Alguien sustrajo criptomonedas (ethereum, la segunda más usada tras bitcoin) por valor de 625 millones de dólares (alrededor de 600 millones de euros) de una web relacionada con el videojuego *Axie Infinity*. Estados Unidos no tardó en relacionar el ataque con el grupo Lazarus, unos ciberdelincuentes de Corea del Norte muy conocidos entre los expertos en ciberseguridad. La consultora especializada en *blockchain* Chainalysis estima que estos *hackers* norcoreanos podrían haberse adueñado el año pasado de otros 400 millones en activos digitales a través de varios ataques dirigidos a plataformas de criptomonedas.

Muchos países, como China, Irán o EE UU, patrocinan extraoficialmente a equipos de *hackers* para que realicen sabotajes o consigan información de valor. El caso de Pyongyang es distinto: utiliza a su grupo de expertos informáticos para hacer dinero. El Amado y Respetado Líder (esa es una de las formas oficiales de referirse a Kim Jong-un) lo ve como una vía para sobrevivir a las duras sanciones internacionales a las que está sometido el régimen.

Calificar a Lazarus de simples rateros digitales sería menospreciarlos. Su hoja de servicios está al alcance de muy pocos. EE UU y Reino Unido, así como Microsoft, les atribuyen el lanzamiento en 2017 de WannaCry 2.0, el mayor *ransomware* de la historia, que acaba de cumplir cinco años. Esta modalidad de virus informático secuestra los equipos infectados y los libera tras el pago de un rescate. Se calcula que WannaCry afectó a unos 300.000 ordenadores de 150 países, incluyendo los del sistema de salud de Reino Unido, que quedó paralizado.

Un año antes, en 2016, Lazarus intentó robar 1.000 millones de dólares al Banco Central de Bangladesh con un sofisticado plan que incluía hacerse pasar por empleados de la entidad y lograr permisos para mover el dinero. El ataque se vio frustrado por un error de codificación, pero no antes de hacerse con 81 millones. El FBI lo consideró entonces el mayor ciberatraco de la historia. Existen sospechas también de que en 2018 robaron unos 530 millones de dólares en *tokens (*fichas digitales) del portal japonés de intercambio de criptomonedas Coincheck.

Hacer dinero para el Líder

Todo el dinero que gana Lazarus tiene un mismo destinatario: el régimen de Kim Jong-un. Lazarus es una rareza en el mundo de las amenazas persistentes avanzadas (APT en sus siglas inglesas), término con el que se conoce a los grupos organizados de *hackers* con mayores capacidades. Estos equipos, dirigidos y patrocinados extraoficialmente por gobiernos, se encuentran en la cúspide de la pirámide de los *hackers*. Están muy bien estructurados y jerarquizados —cuentan con departamentos y profesionales con roles muy definidos— y disponen de recursos económicos, lo que les permite elaborar ataques complejos, coordinados y veloces. Sobre el papel, solo los servicios secretos de las grandes potencias (EE UU, Rusia o Reino Unido) tienen más poder que las APT.

Debido a la propia naturaleza de internet, donde es sencillo pasar desapercibido, los ciberataques son muy difíciles de atribuir. “Las APT son rastreadas básicamente con pistas aportadas por los servicios de inteligencia y particularidades del código, pero hacer un buen análisis forense que determine la autoría puede llevar meses”, explica el *hacker* y analista de ciberseguridad Deepak Daswani. Por eso, los gobiernos usan las APT para sabotear, espiar o llevar a cabo acciones de inteligencia sin provocar incidentes diplomáticos.

“El de Lazarus es un caso único”, subraya Adam Meyers, responsable de inteligencia de CrowdStrike y experto en APT. “Otros grupos lanzan *ransomware*, como Rusia en Ucrania a través de Voodoo Bear, pero como tapadera para otros fines, sin interés alguno en ser pagados. Y si hacen dinero es para su propio beneficio, como las mafias. El objetivo de Lazarus es conseguir fondos para sostener un régimen asfixiado por las sanciones internacionales”, añade el analista tejano.

Fotograma del vídeo distribuido en marzo de este año por Pyongyang en el que Kim Jong-un dirige el lanzamiento de un misil balístico intercontinental.朝鮮通信社 **(AP)**

Lazarus es de hecho la palabra clave que se le dio a los *hackers* que operan desde Corea del Norte. El equipo de Meyers distingue cinco facciones diferenciadas dentro de ese paraguas, con objetivos y especializaciones bien definidas, pero que comparten hasta un repositorio de código al que recurren para preparar sus ataques. Dos de ellos, Stardust Cholima y Labyrinth Cholima, están exclusivamente dedicados a la monetización. "Creemos que Stardust Cholima pertenece a la Oficina 121, uno de los departamentos de la Oficina General de Reconocimiento", nombre con el que se conoce a una de las agencias de espionaje norcoreanas. "Están muy enfocados en sistemas financieros, criptomonedas y nuevas tecnologías".

El entramado de Lazarus también realiza acciones de sabotaje, en la línea de las APT de otros países. Los grupos de *hackers* de Corea del Norte fueron especialmente activos durante los meses de 2020 en los que las grandes farmacéuticas trabajaban frenéticamente para desarrollar una vacuna contra la covid. Trataron de entrar en los ordenadores de trabajadores de AstraZeneca, que junto con la Universidad de Oxford estaban en pleno desarrollo de uno de los remedios. Más tarde intentaron robar información de Pfizer, otro de los laboratorios volcados en la vacuna. Curiosamente, Corea del Norte es de los pocos países del mundo en los que la pandemia se mantuvo a raya (hasta hace unas semanas), por lo que sus intenciones podrían haber sido simplemente torpedear el proceso o vender secretos industriales.

Otro de sus golpes más sonados no perseguía fines económicos, sino venganza. Se desarrolló en 2014 y fue el primer aviso de que los norcoreanos no eran aficionados en el terreno digital. El objetivo fue Sony Entertainment, la productora de *La entrevista*, una película que fantasea con el asesinato de Kim Jong-un. Un mes antes de la fecha de estreno prevista, un grupo de *hackers* infectó los ordenadores de trabajadores de Sony. Consiguieron borrar datos sensibles de la compañía, publicaron detalles salariales y revelaron *emails* comprometedores de algunos de sus directivos. También amenazaron con atentados en las salas de cine donde se exhibiera la cinta, lo que llevó a las grandes distribuidoras a retirarla de la cartelera.

El gran paso adelante de Kim Jong-un

Nadie creía que Corea del Norte sería capaz de convertirse en una potencia cibernética. Tampoco que pudiera desarrollar la bomba atómica. Pero consiguió ambas cosas. Lo segundo fue la obsesión de tres generaciones de dictadores; lo primero, un deseo expreso del actual.

Kim Jong-un dirige con mano de hierro uno de los países más aislados del mundo. Desde que en 2009 tomara el testigo de su padre, supo ver el potencial de la esfera digital tanto para espiar y sabotear a sus enemigos (EE UU y Corea del Sur) como para ganar un dinero que no puede conseguir a través del comercio. "El régimen norcoreano potencia activamente a los *hackers* de élite para incorporarlos a la Oficina 121″, escribe la australiana Anna Fifield en su libro *El gran sucesor* (Capitán Swing, 2021), en el que hace una radiografía de la hermética vida y carrera del nieto de Kim Il-sung. "Los estudiantes que muestran posibles aptitudes en este sentido, algunos de tan solo 11 años, son enviados a escuelas especiales y luego a la Universidad de Automatización de Pyongyang", donde "a lo largo de cinco años se les enseña a *hackear* sistemas y a crear virus informáticos".

Resulta llamativo, cuenta Fifield, que ya en 2018 los estudiantes norcoreanos obtuvieran regularmente los primeros puestos en las competiciones, o *hackatones*, organizadas por la empresa de *software* india CodeChef. Por lo que ha podido averiguar la periodista, buena conocedora del país debido a sus años en Tokio y Pekín como jefa de las oficinas del *Washington Post* y en Corea del Sur como corresponsal del *Financial Times*, los *hackers* norcoreanos gozan de una posición de respeto y una vida acomodada en un país en el que hasta los años noventa la gente moría literalmente de hambre.

Según cuenta Fifield a EL PAÍS, no tiene datos de que en los últimos años haya cambiado su estatus. Más bien al contrario: Kim Jong-un tiene claro que el cibercrimen es un negocio más, una respuesta a las sanciones internacionales. "El régimen participa en todo tipo de sectores que le puedan aportar divisas, como las pruebas farmacéuticas, el cultivo de opio o el tráfico de personas", indica Meyers "El ciberespionaje y el cibercrimen son un vector más". Si no puede ganar dinero comerciando, lo robará.

Referencia Electrónica

Pascual, M. G. (2022, May 23). Lazarus, los cibercriminales que roban y extorsionan para el Amado Líder de Corea del Norte. Ediciones EL PAÍS S.L. https://elpais.com/tecnologia/2022-05-23/lazarus-los-cibercriminales-que-roban-y-extorsionan-para-el-amado-lider-de-corea-del-norte.html