CIBERCRIMEN | UN POCO DE HISTORIA

**El robo de Lazarus por US$ 14 millones que hackers llevaron a cabo en dos horas**

*Lazarus, el misterioso grupo de hackers de Corea del Norte al que acusan de crear el virus WannaCry, ejecutó la extracción de dinero desde cajeros automáticos alrededor del mundo.*

**Por Julián M. Zappia.  
Diplomatic Week.**

En 2018, varios hombres en el estado de Maharashtra, en el noroeste de India, pensaron que estaban en una película, pero en realidad los estaban engañando para que se convirtieran en "mulas de dinero", recolectando efectivo en un ambicioso atraco bancario.

El asalto tuvo lugar durante un fin de semana de agosto de 2018 y se centró en el Banco Cooperativo Cosmos, con sede en Pune, India.

En una tarde de sábado, el personal de la oficina central del banco recibió repentinamente una serie de mensajes alarmantes.

Eran de la compañía de tarjetas de pago Visa, en Estados Unidos, advirtiendo que podría haber miles de demandas por grandes retiros de efectivo en cajeros automáticos, por personas que aparentemente usaban tarjetas del Banco Cosmos.

Pero cuando el equipo del banco revisó sus propios sistemas, no vieron transacciones anormales.

Aproximadamente media hora después, solo para estar seguros, autorizaron a Visa para que detuviera todas las transacciones de las tarjetas bancarias Cosmos. Este retraso resultó extremadamente costoso.

Al día siguiente, Visa compartió la lista completa de transacciones sospechosas con la oficina central de Cosmos: alrededor de 12.000 retiros separados de diferentes cajeros automáticos en todo el mundo. El banco había perdido casi US$ 14 millones.

Fue un crimen audaz caracterizado por su gran escala y su sincronización.

Los delincuentes habían saqueado cajeros automáticos en 28 países diferentes, incluidos Estados Unidos, Reino Unido, Emiratos Árabes Unidos y Rusia.

Todo sucedió en el espacio de solo dos horas y 13 minutos; fue una extraordinaria movilización global organizada y criminal.

Eventualmente, los investigadores rastrearían sus orígenes hasta un oscuro grupo de piratas informáticos que habían llevado a cabo una sucesión de estafas anteriores aparentemente ordenadas por Corea del Norte.

Pero antes de tener una idea más amplia del robo, los investigadores de la unidad de delitos cibernéticos de Maharashtra se sorprendieron al ver imágenes de CCTV de decenas de hombres caminando hacia una serie de cajeros automáticos, insertando tarjetas bancarias y almacenando billetes en bolsos.

Un grupo criminal tenía un encargado que estaba monitoreando las transacciones de los cajeros automáticos en tiempo real en una computadora portátil.

Usando las imágenes de las cámaras de seguridad y los datos de los teléfonos móviles de las áreas cercanas a los cajeros automáticos, los investigadores indios pudieron arrestar a 18 sospechosos en las semanas posteriores al atraco. La mayoría están ahora en prisión, en espera de juicio.

Según la información oficial, estos hombres no eran ladrones. Entre los arrestados había un mesero, un chofer y un zapatero. Otro tenía un título de farmacia.

A pesar de esto, se cree que cuando ocurrió el robo, incluso los hombres reclutados como "extras" sabían lo que realmente estaban haciendo.

Los investigadores creen que el secreto y aislado estado de Corea del Norte estuvo detrás del atraco.

Corea del Norte es una de las naciones más pobres del mundo, pero una parte importante de sus limitados recursos se destina a la construcción de armas nucleares y misiles balísticos, actividad que está prohibida por el Consejo de Seguridad de la ONU.

Como resultado, la ONU ha impuesto importantes sanciones al país, lo que ha hecho que su comercio sea altamente restrictivo.

Desde que llegó al poder hace 11 años, el líder de Corea del Norte, Kim Jong Un, ha supervisado una campaña sin precedentes de pruebas de armas, incluidas cuatro pruebas nucleares y varios intentos provocativos de lanzamientos de prueba de misiles intercontinentales.

**El grupo Lazarus.**

Las autoridades estadounidenses creen que el gobierno de Corea del Norte está utilizando un grupo de piratas informáticos de élite para entrar en bancos e instituciones financieras de todo el mundo para robar el dinero que necesita para mantener a flote su economía y financiar su programa de armas.

Se cree que los hackers, apodados como el Grupo Lazarus, pertenecen a una unidad dirigida por la poderosa agencia de inteligencia militar de Corea del Norte, la Oficina General de Reconocimiento.

Los expertos en seguridad cibernética nombraron a los hackers en honor a la figura bíblica de Lázaro, que regresa de entre los muertos, porque una vez que sus virus ingresan a las redes informáticas, es casi imposible eliminarlos.

El grupo saltó a la fama internacional por primera vez cuando el entonces presidente de EE.UU., Barack Obama, acusó a Corea del Norte de piratear la red informática de Sony Pictures Entertainment en 2014.

El FBI acusó a los piratas informáticos de realizar el dañino ataque cibernético en represalia por "La entrevista", una película cómica que representaba el asesinato de Kim Jong Un.

Desde entonces, el Grupo Lazarus fue sido acusado de intentar robar US$1.000 millones del banco central de Bangladesh en 2016 y de lanzar el ataque cibernético WannaCry que intentó chantajear a organizaciones e individuos en todo el mundo, incluido el Servicio Nacional de Salud de Reino Unido.

Corea del Norte niega enérgicamente la existencia del Grupo Lazarus y todas las acusaciones de piratería informática patrocinada por el Estado.

Pero los principales organismos de seguridad afirman que los ataques de Corea del Norte son más avanzados, más descarados y más ambiciosos que nunca.

**El robo cibercriminal.**

Para el robo del banco Cosmos, los hackers utilizaron una técnica conocida como "jackpotting", llamada así porque hace que el cajero automático “despida” todo su efectivo.

Los sistemas del banco fueron inicialmente comprometidos de la manera clásica: a través de un correo electrónico de "phishing" que abrió un empleado e infectó la red informática con un programa maligno.

Una vez dentro, los hackers manipularon el software, el llamado interruptor de cajero automático, que envía mensajes a un banco para aprobar un retiro de efectivo.

Con esto los piratas informáticos tenían poder para permitir los retiros en cajeros automáticos de sus cómplices en cualquier parte del mundo.

Lo único que no podían cambiar era la cantidad máxima para cada retiro, por lo que necesitaban muchas tarjetas y mucha gente trabajando.

En preparación para el robo, trabajaron con cómplices para crear tarjetas de cajero automático "clonadas", utilizando datos de cuentas bancarias genuinas para crear tarjetas duplicadas que se pueden usar en cajeros automáticos.

La compañía de seguridad británica BAE Systems sospechó de inmediato que era obra del Grupo Lazarus. Los había estado monitoreando durante meses y sabía que estaban conspirando para atacar un banco indio. Simplemente no sabía cuál.

La logística involucrada en el robo al Cosmos es asombrosa.

Los investigadores de seguridad tecnológica de EE.UU. creen que el Grupo Lazarus conoció a un facilitador clave en la web oscura, donde hay foros completos dedicados a intercambiar habilidades de piratería y donde los delincuentes a menudo venden servicios de apoyo.

En febrero de 2018, un usuario que se hacía llamar Big Boss publicó consejos sobre cómo realizar fraudes con tarjetas de crédito.

También dijo que tenía el equipo para hacer tarjetas de cajero automático clonadas y que tenía acceso a un grupo de “mulas de dinero” en Estados Unidos y Canadá.

Este era precisamente el servicio que necesitaba el Grupo Lazarus para su ataque al Banco Cosmos, y comenzaron a trabajar con Big Boss.

Los detectives de seguridad lograron vincularlo con todos estos nombres de usuario, ya que usó la misma dirección de correo electrónico en diferentes foros.

Aquí cometió un grave error.

En 2019, Big Boss fue arrestado en Estados Unidos y descubierta su identidad como Ghaleb Alaumary, un canadiense de 36 años.

Se declaró culpable de delitos que incluyen el lavado de fondos de presuntos atracos bancarios de Corea del Norte y fue sentenciado a 11 años y ocho meses.

Corea del Norte nunca ha admitido ninguna participación en el trabajo del Banco Cosmos, o cualquier otro esquema de piratería.

En febrero de 2021, el FBI, el Servicio Secreto de EE.UU. y el Departamento de Justicia anunciaron cargos contra tres presuntos piratas informáticos del Grupo Lazarus: Jon Chang Hyok, Kim Il y Park Jin Hyok, quienes dijeron que trabajan para la agencia de inteligencia militar de Corea del Norte.

Ahora se cree que residen en Pyongyang.

Las autoridades estadounidenses y surcoreanas estiman que Corea del Norte tiene hasta 7.000 piratas informáticos capacitados.

Es poco probable que todos trabajen desde el interior del país, donde pocas personas tienen permiso para usar internet, lo que dificulta ocultar las actividades de los usuarios. Más bien, a menudo son enviados al extranjero.

Corea del Norte niega haber enviado piratas informáticos al extranjero, solo trabajadores informáticos con visas válidas.

En septiembre de 2017, el Consejo de Seguridad de la ONU impuso las sanciones más estrictas hasta el momento a Corea del Norte, limitando las importaciones de combustible, restringiendo aún más las exportaciones y exigiendo que los países miembros de la ONU enviaran a los trabajadores norcoreanos a su país para diciembre de 2019.

Sin embargo, los piratas informáticos todavía parecen estar activos. Ahora estarían apuntando a empresas de criptomonedas y se estima que han robado, hasta el momento, cerca de US$ 3.200 millones.

Las autoridades estadounidenses los han llamado "los principales ladrones de bancos del mundo", que utilizan "teclados en lugar de armas".