Fuente:
Tomado del periódico Granma

Los ciberataques orquestados contra sitios web cubanos se ejecutaron con el empleo de direcciones IP registradas en proveedores de servicios de telecomunicaciones de Estados Unidos, Reino Unido, Francia, Turquía, Alemania y Países Bajos. En exclusiva para Granma, ofreció declaraciones el director de la Oficina de Seguridad para las Redes Informáticas.

A la par de la campaña mediática y de las noticias falsas (fake news), que se ha generado contra Cuba en el espacio virtual, el Primer Secretario del Partido y Presidente de la República, Miguel Díaz-Canel Bermúdez, denunció que «estamos bajo el fuego sofisticado de una ciberguerra».

Desde el 12 de julio último y hasta la fecha, se intensificó la ocurrencia de incidentes de ciberseguridad, que han afectado la disponibilidad de varios sitios web gubernamentales entre ellos el de la Presidencia de Cuba, y el del Ministerio de Relaciones Exteriores. También han sido atacados los pertenecientes a medios de prensa nacionales como los portales del periódico Granma y Cubadebate, así como los de varios organismos e instituciones.

De acuerdo con Miguel Gutiérrez Rodríguez, director general de la Oficina de Seguridad para las Redes Informáticas (OSRI), un ciberataque es una acción que se ejecuta con intencionalidad, incluso en su modalidad simulada para identificar y solucionar vulnerabilidades como defensa proactiva.

En primer lugar, estos ataques congestionan los canales de comunicación y afectan la calidad del servicio de acceso a Internet, motivando molestias e insatisfacciones en los clientes.

Estos incidentes indican que en el ámbito de la ciberseguridad es necesario trabajar permanentemente en la identificación y eliminación de las brechas de seguridad en las infraestructuras y los sistemas informáticos, continuar promoviendo una cultura de seguridad tecnológica, elevar la percepción de riesgo y estimular el uso responsable de las tecnologías.

Para atender estos sensibles asuntos, el país tiene implementado un sistema de trabajo, que concibe la notificación periódica de vulnerabilidades a las instituciones de la Isla, con el objetivo de que actualicen sus sistemas de seguridad y protección tecnológica, en interacción con las entidades especializadas.

CIBERATAQUES DETECTADOS

De acuerdo con Gutiérrez Rodríguez en lo fundamental se han detectado ciberataques de denegación de servicios, conocidos como DoS/DDoS, según sus características.

En términos generales, se generan muchas solicitudes a un servidor hasta que exceda su capacidad de procesamiento y colapse, atentando contra la disponibilidad de los sitios web en internet, al ponerlos fuera de línea.

El Director General de la OSRI precisó a Granma que, en estos días han sido descubiertos ciberataques orientados a tomar el control de las bases de datos de los sitios web y obtener información de valor (conocidos como inyección SQL) y crear condiciones para mantener dicho control en el tiempo.

Afirmó que, aunque no se ha detectado, es práctica en los ciberatacantes tratar de tomar el control de los servidores, incrementando la peligrosidad de la acción contra nuestros sistemas informáticos.

Con respecto a los lugares desde los cuales proviene esta agresión, detalló que aunque «es posible identificar las direcciones IP desde las que se ejecutan las acciones nocivas contra el país, eso no necesariamente significa que intencionalmente esa nación ataque a Cuba».

En la actualidad, dijo, existen tecnologías que operan, burlando las medidas de ciberseguridad y utilizan los recursos de internet de un Estado sin que sea de su conocimiento, para agredir a terceros países.

Explicó que los ciberataques a los sitios web antes mencionados, fundamentalmente, se ejecutaron con el empleo de las direcciones IP registradas en proveedores de servicios de telecomunicaciones de Estados Unidos de América, Reino Unido, Francia, Turquía, Alemania y Países Bajos.

Acciones de este tipo se contraponen a los esfuerzos del Gobierno cubano por el desarrollo de las telecomunicaciones, las que aun con sus limitaciones tienen un carácter inclusivo y constituyen un eje para el desarrollo estratégico de la nación.

En los últimos años este avance informático ha tenido un marcado crecimiento, apreciado por la población en la comunicación con sus familiares, y en la facilitación de la formación profesional, el entretenimiento, el teletrabajo y trabajo a distancia, así como en el empleo del gobierno y el comercio electrónicos.

ACCIONES ADOPTADAS DESDE CUBA

Siempre que se detecta un incidente de ciberseguridad, comentó Gutiérrez Rodríguez, se inicia una acción coordinada en la que participan múltiples actores, incluyendo las entidades que son afectadas.

De hecho, puntualizó, «todas las instituciones se implican, debido a que se emiten alertas de ciberseguridad con el objetivo de incrementar las medidas de monitorización para mantener la ciberseguridad en los servicios e infraestructuras del país».

Las principales acciones que se ejecutan, son las siguientes:

-Eliminar o mitigar, según existan las condiciones, las vulnerabilidades detectadas en los sistemas, tanto por las entidades y estructuras especializadas en ciberseguridad como por las propias instituciones responsables de los sitios web.

-Reforzar las medidas organizativas y técnicas en las plataformas informáticas y dispositivos de seguridad, que protegen las redes de telecomunicaciones.

-Ejecutar acciones técnicas con el objetivo de contener el avance de los ciberataques.

-Remitir reclamaciones internacionales desde el Equipo de Respuesta a Incidentes Computacionales de Cuba (CuCERT) a organizaciones similares en cada país, donde se encuentran registradas las direcciones IP, que se utilizaron para ejecutar los ciberataques.

El Director General de la OSRI señaló que, ante la aparición de vulnerabilidades desconocidas, se colabora con centros, entidades especializadas y universidades en busca de soluciones, a partir de procesos de investigación e innovación, cuyos resultados se introducen con inmediatez en los esquemas de seguridad de las redes informáticas.

En estos momentos, añadió, se realizan los procesos investigativos correspondientes para determinar las responsabilidades e implicaciones, así como se llevan a cabo las reclamaciones internacionales a los Equipos de Respuesta ante Emergencias Informáticas o los Centros de Respuesta a Incidentes de Seguridad Cibernéticos de cada país involucrado en estos lamentables hechos.

Una vez concluido el proceso, explicó Gutiérrez Rodríguez, se aplicarán las medidas administrativas en los casos que sea necesario, y el régimen contravencional previsto.

Además, se evalúa la pertinencia de realizar denuncias internacionales sobre estos eventos, dado que ocurren en un período en el que se intenta desestabilizar el país y, por consiguiente, forman parte de acciones coordinadas para hacer colapsar la visibilidad del Gobierno cubano y sus instituciones en internet, nuestra credibilidad y la difusión de información, a través de medios oficiales respecto a la situación real que se vive en la nación.

Cuba no se quedará callada ante los ciberataques financiados y fomentados por el imperialismo norteamericano, los denunciará ante el mundo y adoptará las medidas necesarias para enfrentarlos.

CRONOLOGÍA DE LOS INCIDENTES DE CIBERSEGURIDAD

12/07/2021

-Ministerio de Relaciones Exteriores en los sitios web www.cubaminrex.cu [1] y www.cubavsbloqueo.cu [2]

15/07/2021

-Banco Central de Cuba (www.bc.gob.cu [3])

16/07/2021

Servicio de hospedaje de Etecsa, que afectó varios sitios web, entre los que se destacan:

- Presidencia de la República (www.presidencia.gob.cu [4])

- Periódico Granma (www.granma.cu [5])

- Cubadebate (www.cubadebate.cu [6])

- Instituto Cubano de Radio y Televisión (www.icrt.gob.cu [7])

- Tribunal Supremo Popular (www.tsp.gob.cu [8])

- Partido Comunista de Cuba (www.pcc.cu [9])

- Contraloría General de la República (www.contraloria.gob.cu [10])

- Ministerio de Comercio Exterior y la Inversión Extranjera (www.mincex.gob.cu [11])

- Aduana General de la República (www.aduana.gob.cu [12])

- Instituto de Planificación Física (www.ipf.gob.cu [13])

- Fiscalía General de la República (www.fgr.gob.cu [14])

- Ministerio de Educación (www.mined.cu [15])

17/07/2021

-Biocubafarma (www.biocubafarma.cu [16])

(Fuente: OSRI)

Links
[1] http://www.cubaminrex.cu
[2] http://www.cubavsbloqueo.cu
[3] http://www.bc.gob.cu
[4] http://www.presidencia.gob.cu
[5] http://www.granma.cu
[6] http://www.cubadebate.cu
[7] http://www.icrt.gob.cu
[8] http://www.tsp.gob.cu
[9] http://www.pcc.cu
[10] http://www.contraloria.gob.cu
[11] http://www.mincex.gob.cu
[12] http://www.aduana.gob.cu
[13] http://www.ipf.gob.cu
[14] http://www.fgr.gob.cu
[15] http://www.mined.cu
[16] http://www.biocubafarma.cu