ARMADA DE COLOMBIA

CENTRO INTERNACIONAL DE INVESTIGACIÓN Y ANÁLISIS CONTRA NARCOTRÁFICO MARÍTIMO

ANÁLISIS DE COYUNTURA 013

CIBERDELINCUENCIA, UN ACTO EN DETRIMENTO DEL COMERCIO MARÍTIMO

DICIEMBRE - 2023

CENTRO INTERNACIONAL DE INVESTIGACIÓN Y ANÁLISIS CONTRA NARCOTRÁFICO MARÍTIMO
CARTAGENA - COLOMBIA

APROXIMACIÓN DE LA DINÁMICA DEL NARCOTRÁFICO A NIVEL REGIONAL

INTEGRACIÓN REGIONAL, ANÁLISIS E INNOVACIÓN

Protegemos el azul de la bandera

Colombia - Brasil - Ecuador - Guatemala - Honduras - México - Panamá - Perú - Rep. Dominicana

SITUACIÓN COYUNTURAL:

Narco usa a hackers para enviar cargamentos de droga a Europa

Los hackers ingresan a los sistemas informáticos de los dos puertos más grandes de Europa y venden información a los cárteles para enviar droga sin que sea interceptada por las autoridades. Los cárteles del narcotráfico han sofisticado los métodos que utilizan para traficar drogas a distintos países sin que sean detectados por las autoridades y de esa manera los cargamentos puedan llegar a su destino final sin complicaciones.

El uso de hackers es una de las estrategias que han implementado para acceder a los sistemas informáticos de los puertos europeos y de esa forma controlar la llegada de embarcaciones cargadas con estupefacientes, como cocaína.

¿Puede presentarse esta situación en los puertos marítimos de América Latina?

1. ANÁLISIS GENERAL DEL ESCENARIO.

El 5 de julio del año 2017 la Organización Marítima Internacional (OMI), tras haber tomado en consideración la necesidad urgente de elevar el nivel de concienciación sobre las amenazas y las vulnerabilidades conexas con los riesgos cibernéticos, aprobó las **DIRECTRICES SOBRE LA GESTIÓN DE LOS RIESGOS CIBERNÉTICOS MARÍTIMOS**; estas Directrices facilitan recomendaciones de alto nivel sobre la gestión de los riesgos cibernéticos marítimos para proteger el transporte marítimo de los riesgos cibernéticos y las vulnerabilidades, tanto existentes como emergentes, también recogen elementos funcionales para apoyar una gestión efectiva de los riesgos cibernéticos.

El riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posibles, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas (OMI, 2017).

Ante lo anteriormente descrito, hackers obtuvieron acceso a sistemas informáticos en dos de los puertos más grandes de Europa y vendieron mensajes a los cárteles de la droga para que pudieran transportar drogas sin ser interceptados por las autoridades. En el caso generador de este análisis, los hackers se infiltraron en los Puertos de Rotterdam y Amberes, los sistemas portuarios más grandes de Europa, y vendieron inteligencia a los narcotraficantes.

Este hecho investigado recientemente, pone en alerta a las autoridades marítimas en virtud que estas acciones también podrían estar ocurriendo en puertos de todo el mundo, enfocándose principalmente en aquellos territorios con dinámicas delictivas de producción, tránsito y/o consumo de sustancias ilícitas.

Los cárteles de la droga utilizan métodos sofisticados para transportar droga a diferentes países sin ser detectados por las autoridades para que la mercancía llegue a su destino. En este contexto, el uso de hackers es una de las estrategias que los cárteles vienen implementando para acceder a los sistemas informáticos en los puertos europeos y así acceder a información de cargas, naves y tripulaciones con el fin de controlar la llegada de potenciales medios de tráfico con estupefacientes.

Gracias a la digitalización y el "internet de las cosas"[1] del transporte marítimo, los cárteles que intentan traficar drogas bajo la modalidad de "Contenedores" ya no tienen que crear extensas cadenas de corrupción, cada vez más identificadas y contenidas por las autoridades, encontrando una oportunidad estratégica en los altos niveles de automatización de la infraestructura portuaria.

Los Hackers tiene algunas capacidades ilegales de interés, como las que se detallan a continuación:

- Monitorear cómo se escanean los contenedores, por lo que "asesoran" a los narcotraficantes sobre cómo colocar las drogas en los contenedores potencialmente atractivos, para evitar ser detectados.
- Infectar el sistema informático del puerto con un malware, permitiéndoles obtener información sobre los envíos de contenedores y modificarla para facilitar su extracción.
- Cancelar el servicio de recogida original de un contenedor y falsificar documentos para que su cliente pudiera recoger el contenedor, sacarlo del puerto y descargar la droga.
- Identificar rutas de envío menos controladas y compartir estos datos con delincuentes organizados para cargar drogas en contenedores sin el conocimiento de las compañías navieras.
- Monitorear el historial de escaneos de las compañías que regularmente envían contenedores a un puerto para recomendar qué líneas de transporte marítimo se caracterizan por tener menos controles.
- Acceder al contenedor usando código de acceso (PIN), con la colaboración de empleados portuarios en la mayoría de las veces. El PIN le permite no sólo recoger el contenedor, sino también rastrearlo en el puerto hasta que esté listo para recogerlo.
- Crear código para contenedores utilizando malware.

Estos ataques hackers pueden ser aplicados contra:

a) Computadores y sus redes.
b) Informaciones almacenadas.
c) Servicios esenciales.
d) Infraestructuras, cómo puertos, entre otros.

2. POSIBLES CAUSAS

Las tecnologías cibernéticas se han convertido en esenciales para el funcionamiento y la gestión de los numerosos sistemas cruciales para la seguridad y la protección del transporte marítimo, y la protección del medio marino. En algunos casos, estos sistemas han de cumplir las normas internacionales y las prescripciones de las Administraciones de abanderamiento. No obstante, la vulnerabilidad generada por el acceso, la interconexión o el establecimiento de redes entre estos sistemas puede dar lugar a riesgos cibernéticos que deberían abordarse.

La guerra cibernética es el resultado de avances tecnológicos y la instrumentalización de la infraestructura técnica de la globalización (Globalización Desviada), con fines ilegales, que para el

[1] El Internet de las cosas (IoT) es un término que se refiere a la red de dispositivos físicos que están conectados a Internet. Estos dispositivos están equipados con sensores, software y conectividad de red que les permite recopilar y compartir datos.

caso del narcotráfico, brindan una capacidad ilegal anticipativa con bajos niveles de riesgo y altos índices de certeza en la información traficada.

Comprender las intenciones y los patrones de comportamiento de los ciberdelincuentes es parte de todos los conflictos de la historia moderna y es una de las armas más poderosas en cualquier guerra. Pero en la era del internet, la información fluye en tiempo real, dándole mayor sentido de complejidad y avance al entorno tecnológico de la infraestructura portuaria analizada. Hoy en día, el frente cibernético desempeña un papel crucial en el desarrollo e incluso en el resultado de un conflicto, y parece complementar los ejercicios militares sobre el terreno. La guerra contra el narcotráfico no se escapa de estas variables.

Los Estados están invirtiendo cada vez más en entidades que operan en el ciberespacio. Sin embargo, incluso las superpotencias tendrán cierta vulnerabilidad a los ciberataques, ya que las vulnerabilidades surgirán a medida que la virtualización y la digitalización de la información se consoliden. Este es un nuevo campo de batalla donde grupos de hackers de diferentes países luchan para medir sus fuerzas contra las autoridades. Sin embargo, estos actores no operan en el vacío y tienen relaciones, aunque no formales, con países y con organizaciones criminales transnacionales, como es el caso del narcotráfico internacional.

Para obtener ventajas y, por supuesto altas ganancias, los ciberdelincuentes que delinquen a favor del narcotráfico planean ataques a infraestructuras utilizadas para el envío y/o movilización de sustancias ilícitas, a través de puertos marítimos.

Se constituye en una imperante necesidad para la inteligencia naval, la identificación y caracterización de actores y capacidades cibernéticas del crimen organizado. La naturaleza real de las organizaciones cibercriminales varía según el nivel de tecnología digital y de red involucrada, la naturaleza de sus operaciones y el público objetivo de sus víctimas, lo que también ayuda a diferenciarlas.

A medida que los puertos experimentan una transformación digital y que utilicen nuevas tecnologías de la información, estarán más conectados, posibilitando a la vez el acceso a más datos. Pero si bien esto tiene muchas ventajas, también facilita los ataques cibernéticos, que se centran en las vulnerabilidades que los sistemas informáticos pueden tener.

Las principales posibles causas de los ciberataques a puertos son:

- Una vulnerabilidad de un sistema informático es un mal funcionamiento o defecto que pone en riesgo los activos porque no están protegidos eficazmente.
- Un empleado filtra accidentalmente información confidencial.
- Los dispositivos electrónicos que almacenan información privada de la empresa portuaria se pierden y son robados.
- Los empleados maliciosos y sin escrúpulos ponen en riesgo la información.
- Las vulnerabilidades de terceros o la falta de control significan que los ciberdelincuentes pueden obtener información de otras empresas portuarias con las que tienen relaciones y encontrar las mismas formas de aprovecharla para el narcotráfico.
- La ingeniería social generalmente implica manipular a ciertas personas para obtener datos confidenciales, como contraseñas u otros datos importantes y relevantes.

Por lo general, al llevar a cabo estos ataques, los ciberdelincuentes intentan obtener información relevante que pueda colaborar con la logística del narcotráfico. Por ello, es importante entender cuáles pueden ser los principales ciberataques para saber actuar de forma rápida, inteligente y poder mitigar el impacto.

Lo primero que hay que recordar es que estos ataques pueden ser externos o internos al ambiente portuario, y sí, en algunos casos los empleados pueden atacar voluntariamente a la empresa portuaria mediante la influencia de actores o integrantes de estructuras ilegales.

Los ciberataques más comunes de los que pueden ser víctimas los puertos marítimos son:

- ***Phishing y Spear Phishing***. El *phishing* implica correos electrónicos o mensajes de texto que parecen provenir de una fuente confiable y convencen al destinatario de realizar una acción o abrir un enlace malicioso que podría comprometer información personal o comercial. El propósito del *Spear phishing* es ganarse la confianza de una persona o empresa en particular y luego utilizarla para obtener datos valiosos. Este ataque es ampliamente utilizado por empresas e individuos conocidos.
- ***Whaling* o "caza de ballenas"**. Se dirigen a ejecutivos como directores ejecutivos o directores financieros y otros puestos de alto nivel en las organizaciones para robar información confidencial a la que tienen acceso.
- ***Malware***. Es un programa o código malicioso que afecta de forma encubierta y silenciosa a los sistemas de información. El *malware* puede invadir, dañar y desactivar computadoras y otros activos de información, lo que significa que puede robar y eliminar datos, secuestrar funciones y monitorear actividades sin que nadie se dé cuenta. Algunos programas maliciosos incluyen *ransomware*, troyanos y software espía. Muy empleado por los hackers para invadir puertos.
- ***Ransomware***. También conocido como secuestro de datos, implica que los hackers bloqueen dispositivos electrónicos y cifren archivos para que el propietario-usuario no pueda acceder a la información y los datos almacenados.
- **Inyección SQL**. Este es un tipo de ciberataque que implica explotar errores y vulnerabilidades en páginas web para infiltrar código malicioso. Se utiliza para robar bases de datos, manipular información o destruirla.

Para evitar que se produzcan amenazas o riesgos cibernéticos a los puertos, es importante implementar bajo el liderazgo de la inteligencia naval y sus capacidades cibernéticas, el análisis de la situación actual e infraestructura tecnológica de las instalaciones portuarias, al tiempo que se identifican actores, funciones y activos vulnerables, con el fin de orientar estrategias de mitigación, capacitación y concientización en seguridad informática y seguridad de redes, para los operadores de la organización, quienes son considerados el eslabón más débil de la cadena.

3. ESCENARIOS FUTUROS.

Con relación a la información proporcionada en la “Evaluación Situacional de la Dinámica del Narcotráfico Marítimo” desarrollado por el CMCON, en el control y seguimiento al entorno regional y a nivel global, se evidencian una multiplicidad de hechos que contribuyen bajo un análisis prospectivo, a configurar posibles escenarios futuros con la finalidad de obtener una adecuada capacidad de respuesta ante la amenaza cambiante, adaptativa y resiliente del narcotráfico y sus delitos conexos que afectan a los Estados.

Los siguientes factores están relacionados en este diagnóstico y tienen correlación con el tema en estudio:

- Fortalecimiento de la Dark web como espacio virtual de tráfico de drogas en América, Europa y Ásia.
- Persistencia en la infiltración de puertos europeos por parte del Organizaciones Criminales Transnacionales (OCT).
- Incremento del poder corruptor de las OCT sobre autoridades europeas, principalmente portuarias.
- Persistencia en la contaminación de contenedores como principal medio de tráfico de América hacia Europa.
- Fortalecimiento de alianzas criminales entre OCT latinoamericanas y europeas.

A partir de los factores de cambio descritos, es posible que se desarrollen los siguientes escenarios de corto y mediano plazo en tema propuesto, así:

a. Escenario Probable de Corto Plazo.

- Podría facilitar la cooperación internacional armonizando, donde sea necesario, los instrumentos bilaterales, regionales y multilaterales sobre delitos cibernéticos.
- Podría adherirse o ratificar los instrumentos regionales y multilaterales sobre delitos cibernéticos para hacer que sean jurídicamente vinculantes.
- Las OCT podría utilizar o incrementar modalidades de ciberataques en los puertos de Centro y Sur América, que, a primera vista, pudieran presentar escenarios de seguridad vulnerables, debido a la implementación de poca tecnología en aspectos de ciberseguridad; aunque la OMI haya efectuado algunas recomendaciones en este aspecto, en la mayoría de veces el mayor impedimento es el recurso económico, que muchas veces se mira como un gasto oneroso y a la vez innecesario.

b. Escenario Probable de Mediano Plazo.

- Incremento de acciones de ciberdelincuentes en todo el mundo podría representar un problema de consideración a futuro, poniendo en riesgo la seguridad de infraestructuras críticas de países a otras amenazas.

Referencias Bibliográficas

BugHunt. (20 de 4 de 2023). *BugHunt*. Obtenido de https://blog.bughunt.com.br/o-que-e-guerra-cibernetica/

InSightCrime. (23 de 11 de 2023). *InSightCrime*. Obtenido de https://insightcrime.org/es/investigaciones/narcofiles-nuevo-orden-criminal/

Jiménez, M. (2 de 3 de 2022). *Pirani*. Obtenido de https://www.piranirisk.com/es/blog/ataques-ciberneticos-causas-y-consecuencias

OMI. (5 de 7 de 2017). *Organizacion Maritima Internacional*. Obtenido de https://www.imo.org/es/OurWork/Security/Paginas/Cyber-security.aspx

RadioFórmula. (9 de 11 de 2023). *Radio Fórmula.mx* . Obtenido de https://www.radioformula.com.mx/mundo/2023/11/9/narco-usa-hackers-para-enviar-cargamentos-de-droga-europa-789236.html

ARMADA DE COLOMBIA

Centro Internacional de Investigación y Análisis Contra Narcotráfico Marítimo

Diagonal 20. Transversal 52
Escuela Naval de Cadetes "Almirante Padilla"
Barrio "El bosque". Isla "Manzanillo"
Cartagena de Indias D.T. y C. (Colombia)
Móvil (+57) 310 7954642
direccion@cimcon.mil.co

Protegemos el azul de la bandera

Colombia - Brasil - Ecuador - Guatemala - Honduras - México - Perú - Rep. Dominicana