MILENIO

Milenio Diario
Sección: Portada, Justicia
2025-04-25 03:16:15 564 cm^2 Página: 1, 4 - 5 1/2

Crimen. Grupos delincuenciales reclutan a jóvenes expertos en informática para atacar plataformas de SSPC, Inteligencia y fuerzas armadas; solo en Sedena reportan 27 intentos al día, aunque fallidos

CJNG lanza a *hackers* contra el sistema de seguridad del Estado

XAVIER JIMÉNEZ, CIUDAD DE MÉXICO

Autoridades mexicanas investigan a una red de *hackers* ligada al *narco* que busca penetrar los sistemas de dependencias de seguridad nacional y Pemex.

"Se indaga a células del CJNG que reclutan a personas expertas en sistemas, ya sea bajo amenazas o como parte de este conglomerado criminal", confirmó a MILENIO un mando militar. PAGS. 4 Y 5

CJNG lanza *hackers* contra el sistema de seguridad del Estado

Ciberataques. Grupos delincuenciales reclutan a jóvenes expertos en informática para penetrar plataformas de SSPC, Inteligencia, fuerzas armadas y hasta Pemex; solo la Sedena registró 27 intentos al día durante el año pasado, aunque fallidos

XAVIER JIMÉNEZ
CIUDAD DE MÉXICO

El gobierno mexicano investiga a una red de *hackers* ligados al Cártel de Jalisco Nueva Generación (CJNG) que busca penetrar, además de los sistemas financieros, los de instancias como la Secretaría de Seguridad y Protección Ciudadana, el Centro Nacional de Inteligencia, las fuerzas armadas y organismos estratégicos como Petróleos Mexicanos, revelaron autoridades militares.

Investigaciones refieren que grupos criminales reclutan a jóvenes expertos en sistemas para *hackear* dichas plataformas mediante intentos de escaneo de vulnerabilidades, de intrusión (inyección de códigos maliciosos), *phishing* (envío de un correo electrónico por parte de un ciberdelincuente simulando ser una entidad legítima) y *softwares* maliciosos, entre otros métodos.

"No está descartado, hay investigaciones abiertas incluso contra células de este grupo (CJNG), que recluta a personas expertas en el manejo de sistemas, ya sea bajo amenazas o como parte de este conglomerado criminal", detalló a MILENIO un mando militar que conoce sobre la problemática.

Sin embargo, advirtió que a pesar de los miles de intentos de penetración, la Secretaría de la Defensa Nacional (Sedena) no registra afectaciones en su estructura informática debido a constantes programas y actualizaciones para la "conten-

ción de ataques cibernéticos".

De 2021 a 2023, la Defensa registró un aumento de 529 por ciento en el número de ataques cibernéticos, al pasar de 6.2 a 39 registros cada 24 horas.

Para 2024, el Ejército registró 27 intentos de intrusión al día, de acuerdo con cifras oficiales.

Los intentos de intrusión y el *phishing* son las herramientas más recurrentes de los *hackers* para intentar penetrar el sistema de la Defensa.

Sin embargo, la institución armada posee programas informáticos de prevención para evitar la propagación de los "incidentes", posteriormente emplea una erradicación de las "causas raíz" (principalmente *malwares*) y después lleva a cabo la recuperación de "incidentes cibernéticos", que consiste en la restauración de los sistemas afectados a su funcionamiento normal.

En sus investigaciones o forensia digital, la Defensa también ha detectado *malwares* como troyanos, botnets y *banking*.

En cuanto a la Secretaría de Marina, entre 2018 y 2024 promediaron 4 mil 600 intentos de ataque al día, de los cuales todos fueron bloqueados.

En abril de 2024 la Interpol señaló al CJNG de estar involucrado en la comisión de fraude financiero mundial mediante uso de tecnología de punta.

"El uso de la Inteligencia Artificial, los grandes modelos de lenguaje y criptomonedas combinados con los modelos de negocios de *phishing* y *ransomware* como servicio han resultado en fraudes más sofisticados y profesionales sin la necesidad de habilidades técnicas avanzadas y a un costo relativamente bajo.

"Cada vez hay más pruebas de que los grupos criminales latinoamericanos como Comando Vermelho (Brasil), Primeiro Comando da Capital (Brasil) y Cártel Jalisco Nueva Generación también están involucrados en la comisión de fraudes financieros", advirtió la Interpol.

El Gabinete de Seguridad, incluido el Centro Nacional de Inteligencia, con el apoyo de la Fiscalía General de la República, dan seguimiento al rastreo de los *hackers*, añadió el mando militar.

Apuntó que cada dependencia cuenta con unidades de Infraestructura Informática y Vinculación Tecnológica, y de Gestión de Servicios, Ciberseguridad y Desarrollo Tecnológico, así como con el Centro Nacional de Información Plataforma México, que poseen información sensible como la identidad de funcionarios, planeación de operativos, número de elementos y proyecciones de seguridad.

Con información de: Rubén Mosso

Entre 2018 y 2024 hubo 4, 600 incidentes diarios sin éxito contra Marina