



PERIÓDICO	PAGINA	FECHA	SECCIÓN
<b>EXCELSIOR</b>	1,1,6D	06/10/2022	LEGISLATIVO

**DINERO**

### Más hackers vulneraron a Sedena

Guacamaya reveló que no son los únicos con acceso a documentos militares, por lo que la institución debe reforzar su ciberseguridad, urgió un especialista. / 6



Foto: Freepik

### ALERTAN A LA SEDENA

Expertos en temas de ciberseguridad afirman que los Guacamaya no fueron los primeros en vulnerar a la Sedena y hay más ataques > 6

## ANTE POSIBLES NUEVOS ATAQUES

SEDENA  
DEBE ESTAR  
EN ALERTA  
MÁXIMA

**GUACAMAYAS NO FUERON LOS PRIMEROS** en vulnerar a la secretaría y expertos aseguran que vendrán más filtraciones



POR AURA HERNÁNDEZ  
aura.hernandez@gimm.com.mx

**E**l grupo Guacamaya aseguró que no es el único que ha tenido acceso a los servidores de la Secretaría de la Defensa Nacional (Sedena), por lo que es necesario que el organismo refuerce de manera inmediata sus medidas de ciberseguridad para evitar próximos ataques.

Los primeros indicios de una posible vulneración del organismo a cargo del general Luis Cresencio Sandoval se dieron el pasado 19 de septiembre, pero no fue hasta que el medio *Latinus* lanzó una nota sobre la fuga de información a finales de ese mes que se tomó en cuenta.

Para Hiram Alejandro Camarillo, director de información de Seekurity, hasta ahora las autoridades han tratado de mitigar el impacto de este caso diciendo que la información filtrada es pública. Sin embargo, demuestra que se necesita tomar acciones para mejorar la ciberseguridad de la Sedena.

Al platicar con **Excelsior**, el especialista de ciberseguridad y uno de los primeros en detectar que la Sedena podría ser víctima de Guacamaya, explicó que la vulnerabilidad se debió a que no instalaron los parches

necesarios de un programa enfocado en correo electrónico y colaboración llamado Zimbra.

Guacamaya, que se da a conocer como grupo hacktivista, reveló que usaron una vulnerabilidad en Zimbra para acceder a los servidores, en los cuales estuvieron cerca de un mes sin ser detectados y lograron extraer 6 terabytes de información.

“Ellos (Guacamaya) mencionaban que habían descubierto que a principios de julio había alguien más que ya estaba dentro del servidor, lo que concuerda con investigaciones internacionales que detectaron que este tipo de vulnerabilidad estaba siendo explotada por ciberdelincuentes”, destacó Camarillo.

Ante esto, recomendó a la Sedena hacer una investigación exhaustiva de cuántas personas se conectaron, en qué momento entraron al servidor y si extrajeron más información.

Adicionalmente, recomendó al organismo encargado de la seguridad nacional hacer caso al informe de Auditoría de Cumplimiento a Tecnologías de Información y Comunicaciones realizado por la Auditoría Superior de la Federación (ASF) en el que Sedena sólo cumplía con dos de los 20 controles necesarios.

## Lo que puede pasar

Camarillo agregó que, si es cierto que otros ciberdelincuentes tuvieron acceso, la Sedena y otros organismos del gobierno podrían enfrentarse a próximos ciberataques.

Esto porque los ciberdelincuentes, a diferencia de grupos como Guacamaya, no buscan información que cause algún problema o acción mediática en el país, sino algo que les genere dinero.

Esto significa que si tuvieron acceso al servidor de la Sedena trataron de extraer usuarios

y contraseñas, información para entrar a otras entidades o sistemas, recolectar correos electrónicos para luego realizar ataques de fuerza bruta en éstos y, si lo logran, empezar a buscar más información.

“El punto para estas personas es ir más allá y sacarle provecho vendiendo los usuarios y contraseñas, ya sea de funcionarios públicos o de acceso a servidores”, añadió.

Habrán grupos de ciberdelincuentes que deseen comprarlas porque entonces podrán hacer otro tipo de ataques como ransomware para secuestrar información sensible y pedir un rescate.



Principalmente, los ciberdelincuentes van a tratar de generar dinero con toda la información sustraída.”

“Guacamaya dice que varias personas ya tenían acceso (al servidor), por eso se debe hacer una investigación exhaustiva.”

**HIRAM ALEJANDRO CAMARILLO**  
DIRECTOR DE INFORMACIÓN DE SEEKURITY

Foto: Freenik y Especial



**Hiram Alejandro**  
@hiramcoop

El grupo Guacamaya ha actualizado su blog:

- Subieron documentos de la Sedena accesibles públicamente
- Ellos NO son los únicos

hackers que entraron a los servidores de la Sedena, cuando ingresaron encontraron evidencia que desde el 5 de julio ya alguien tenía acceso

### Secretaría de la Defensa Nacional de México (Sedena)

Terminan sus fichas sobre Efectos sociales con:

Hasta el momento no se tiene conocimiento que mantenga vínculos con integrantes de organizaciones delictivas.

SEEDNA no puede decir lo mismo sobre sí misma.

No hemos tenido tiempo de investigar mucho, pero sí sí hemos subido algunos documentos que pueden ser de interés público, siendo así se ignora cómo de actualizada la SEDENA está investigando como "amenazas a la seguridad nacional" en el de investigar al crimen organizado y otras amenazas reales.

### Explicación del Hackeo

Según los hechos:

Todos los demás NO sabemos fueron descargados con Proxyshell como se ve en el video. Pero SEDENA fue con una vulnerabilidad antigua de Zimbra. Fue simplemente usar un shell para explotar la vulnerabilidad y subir una webshell, y luego usar la webshell para descargar todos los correos de aproximadamente. Ya había muchas otras webshells allí, con fecha desde el 8 de Julio (la fecha parece ser fuertemente controlado con touch) pero también está documentado que en Julio se empezó a explotar muchos servidores de Zimbra) y vimos que otros hackers también estuvieron descargando los correos a la vez.

### Cobertura mediática

• [https://bit.ly/3u0000000/29-Nov-2022](#)

Sobre porque se publicó primero en Latam, si guacamaya respondió:

Una fuente periodística ya tenía la información, lo que pasó es que hubo una investigación de coberturas de última mano. Esto solo tardó unos días en encontrar algunas informaciones más de ARLO. Nos gustaría que todos fueran accesibles a la información, pero en este caso no es posible, ya que hay información que en manos de nuestro país podría poner en riesgo a muchas gente. Sin embargo se comparte con varios periodistas de investigación, que reportaron a OchoGatos o Ciudad Mexicana, nos gusta su política y sus reportajes o no.