La Razón de México
Sección: Portada,México Página: 1,11
2023-07-05 02:32:18 511 cm2 $114,412.56 1/3

Triple *hackeo* a sistemas pone en "estado grave" a Conagua

CRISIS en dependencia a cargo de Germán Martínez (foto) lleva 83 días y siguen sin el control de operaciones; en riesgo de desaparecer archivos de 15 años. **pág. 11**

Van 83 días sin solución

Conagua, en "estado grave" por triple *hackeo*

CRISIS no ha podido ser solucionada y pone en peligro archivos clave de los últimos 15 años; organismo ha tenido un total de cuatro intrusiones, tres de ellas registradas como ataques

Por Claudia Arellano
claudia.arellano@razon.com.mx

Un triple *hackeo* a sus sistemas informáticos ha puesto en "estado grave" a la Comisión Nacional del Agua (Conagua), en una crisis que no ha podido ser solucionada desde hace 83 días, que amenaza con extenderse más tiempo y que hace peligrar archivos clave de los últimos 15 años.

El organismo ha tenido un total de cuatro intrusiones, pero las registradas como ataques son tres, las cuales han puesto en riesgo su base de datos.

La primera que se ejecutó fue registrada el 13 de abril pasado, aunque ocurrió "una intrusión fallida en la última quincena de marzo", lo que quiere decir que desde ese entonces la red intentó ser vulnerada y, aunque en esa ocasión se "intentó, no se logró.

"El sistema se ve afectado a partir del 13 de abril", contó a *La Razón* el ingeniero informático Juan Carlos Leal, familiarizado con fuentes cercanas a la dependencia federal.

Tras el ataque del 13 de abril, se dio un segundo el 27 de abril y el tercero ocurrió aparentemente los primeros días de junio.

Las redes del sistema de la dependencia fueron invadidas por un virus denominado "BlackBite" que, a decir del especialista, "podría dar origen a la desaparición de archivos importantes, incluso de 15 años a la fecha".

Las afectaciones por el *hackeo* a los sistemas informáticos de la Conagua se extenderían por al menos 70 días, de acuerdo con la última advertencia del propio órgano, pero hasta la fecha no se ha recuperado el control en la operación de dichos sistemas, de acuerdo con Leal.

Según una prórroga emitida por la comisión el 12 de junio, la suspensión de trámites y plazos se extendería hasta el viernes 23 de junio, pero ya han pasado 12 días después del vencimiento de ese periodo y no hay informes de que la situación se haya solucionado.

"Los archivos no han quedado del todo saneados; incluso, se alerta a la población para que, en caso de que requieran bajar algún documento, lo hagan de manera segura", dijo el ingeniero.

"Los virus informáticos son un *software* que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático sin el permiso o el conocimiento del usuario, principalmente para lograr fines maliciosos sobre el dispositivo. México tiene que reforzar su seguridad en materia de ciberseguridad; no es un mal menor, aunque a veces se quiera hacer


La Razón
Xóchitl y Creel ya apuntados enfilan baterías contra AMLO y 4T

ver así, pero en este caso específico, dan un plazo en que quedará operante todo el sistema, pero siempre pueden salir vertientes y nuevos ataques", refirió el ingeniero informático.

Asimismo, dijo que los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este mismo. "Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que sólo producen molestias o imprevistos, pero una vez teniendo un ataque, éste puede llevarnos a otro", advirtió.

Desde el 13 de abril no hay acceso a información histórica de la Conagua ni del Servicio Meteorológico Nacional, y no es posible acceder a los archivos al menos de hace 15 años a la fecha. "No siempre se recupera todo, depende de la agresión y el fin con el que se hizo este trabajo de intromisión", expuso el experto.

A pesar de los trabajos implementados para restablecer la operatividad informática en Conagua, subsiste la afectación, por lo que es necesario "que se dé al menos un informe, donde digan sobre una prórroga de esta suspensión, o bien, que informen que quedó reparado el daño, con la finalidad de continuar con las acciones de detección, análisis y contención del impacto del incidente", expuso el ingeniero.

"Los ciberataques son agresiones a instituciones o personas mediante herramientas informáticas, con un objetivo de obtener información confidencial o de propiedad intelectual. Pudo haber sido quien sea y regularmente se requiere de muy poco, pero de mucha estrategia para poder ejecutarlo", comentó.

El especialista de la Universidad Nacional Autónoma de México (UNAM), quien trabaja para una empresa medidora de riesgos a ciberataques, recordó que las intrusiones más famosas incluyen robos de información masiva a Adobe, Aadhaar, Canva, eBay, Dropbox, Equifax, Uber, Yahoo, Facebook, Twitter y MySpace, entre otros.

Sin embargo, un nuevo término acuñado en diferentes gobiernos es el de la "ciberguerra", que ya ha avanzado en ataques a gobiernos, corporaciones de seguridad y hasta ejércitos. WikiLeaks y Anonymous han vulnerado información estratégica de gobiernos e instituciones e incluso ha habido ataques cibernéticos en procesos electorales como en Estados Unidos, por lo que, dijo el especialista, habrá que estar muy alerta en las elecciones del 2024.

"Si se comienza con un órgano administrativo, dependiente de la Secretaría de Medio Ambiente, que fue la primera alerta a Conagua, se debe evaluar toda la red del Gobierno, no sólo la de Conagua. En abril se emitió una primera alerta y la cuarta se dio en junio, alertando que se extendería la suspensión de la red, por el momento, hasta el viernes 23 de junio. Desde entonces, no se sabe nada más, pero es importante dar seguimiento y alertar", indicó.

El especialista dijo que recientemente Conagua reconoció que, a pesar de los esfuerzos realizados, no ha logrado regresar a la normalidad, y que hasta el momento ha sido recuperado 85 por ciento de los archivos históricos.

"Hasta el momento no se ha detectado robo de información y tampoco que el *hackeo* se haya dado desde dichas instalaciones", concluyó el experto de la Universidad Nacional.

EN MÉXICO, este *hackeo* se suma al que han sufrido dependencias del Gobierno como las secretarías de la Defensa Nacional, Infraestructura, Comunicaciones y Transportes, y Pemex.

Eldato

LOS CIBERATAQUES son agresiones a instituciones o personas mediante herramientas informáticas, con un objetivo de obtener información confidencial o de propiedad intelectual. Pudo haber sido quien sea y regularmente se requiere de muy poco, pero de mucha estrategia para poder ejecutarlo

Juan Carlos Leal
Especialista

Virus BlackBite

Esta amenaza provoca las siguientes afectaciones en los sistemas.

TIPO DE AMENAZA:

Ransomware (secuestro de datos), crypto virus, *files locker*

Síntomas:

- No se pueden abrir archivos almacenados en la computadora.
- Los archivos previamente funcionales ahora tienen una extensión diferente (por ejemplo, my.docx.locked).
- Se muestra un mensaje de solicitud de rescate en el escritorio.
- Los ciberdelincuentes exigen pago de un rescate —generalmente en bitcoins— para desbloquear archivos.

MÉTODOS DE DISTRIBUCIÓN:

Archivos adjuntos de correo electrónico infectados, sitios web de torrents y anuncios maliciosos.

Daños:

- Todos los archivos están encriptados y no se pueden abrir sin pagar un rescate.
- Se pueden instalar troyanos adicionales que roban contraseñas e infecciones de *malware* junto con una infección de *ransomware*.