Ataque. Piratas informáticos robaron correos de dependencias como el Heroico Cuerpo de Bomberos, Secretaría de Obras y Servicios, Procuraduría Social, entre muchas otras

Guacamaya. El tamaño del ataque es de casi una cuarta parte del ocurrido con la Sedena en los llamados Guacamaya Leaks

Vulnerados. Ahora fue el Gobierno de la CDMX quien se vio atacado, pese a las advertencias de riesgo. / DALL-E

Chilango Leaks: hackers de Mexican Mafia 'desnudan' al gobierno de CDMX

Ignacio Gómez

El gobierno de la Ciudad de México fue atacado a través de una vulnerabilidad que desde 2019 se advirtió y que, pese a constantes avisos, no se resguardó de manera adecuada. De esta manera, hackers del grupo Mexican Mafia accedieron a alrededor de 2.1 millones de correos confidenciales de más de dos millares de cuentas de servidores públicos.

La inseguridad del sistema fue advertida, desde hace cinco años, por el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), que reportó una vulnerabilidad crítica en la suite de colaboración Zimbra, utilizada por muchas empresas y gobiernos —como el de la capital del país— para operar correos electrónicos, contactos, tareas y almacenamiento general de archivos.

En ese entonces, el Instituto Nacional de Ciberseguridad de España (Incibe) calificó esta vulnerabilidad, nombrada CVE-2019-9670, como crítica y advirtió que una de las versiones de Zimbra presentaba un riesgo de inyección de entidad externa XML (XXE).

En general, el XXE funciona como una puerta trasera por donde un hacker puede colarse en el sistema de correos electrónicos sin permiso. Este tipo de acción puede permitir diversos ataques, como robar información confidencial o incluso tomar el control del sistema.

Así fue como el hacker conocido como *Lord Peña* logró vulnerar los sistemas de seguridad para acceder a un total de 2,300 cuentas de correo electrónico del gobierno de la Ciudad de México, incluyendo diversas dependencias y organismos autónomos bajo el dominio "*cdmx.gob.mx*". Esto le permitió tomar control de las mismas, acceder a los mensajes recibidos y enviados, así como enviar correos electrónicos desde cualquiera de las miles de cuentas comprometidas.

Estas acciones quedaron al descubierto este lunes 1 de abril a través de publicaciones que circularon brevemente en la red social X. En estos mensajes, se compartieron capturas de pantalla de algunas cuentas de correo comprometidas; sin embargo, posteriormente desaparecieron.

Una creciente ola de ciberataques

En las últimas semanas, el seudónimo de *Lord Peña* ha destacado por varios hackeos. Por ejemplo, el pasado 23 de marzo, *Publimetro* informó que este mismo hacker sustrajo más de 2.3 millones de archivos del Ins-

tituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) de la Universidad Nacional Autónoma de México (UNAM). En total, descargó casi un terabyte de información, que incluía datos sensibles como información bancaria.

Apenas dos días después de haberse publicado dicho ataque, *Lord Peña* puso a la venta la base de datos del IIMAS en el sitio web de Breach Forums, un lugar comúnmente utilizado por hackers para comercializar este tipo de información y filtraciones. El hacker fijó un precio de tan solo 500 dólares, aproximadamente $8,300 MXN, para cualquier persona interesada en adquirir la base de datos y utilizarla a su discreción.

Asimismo, según lo reportado por *Publimetro* el 28 de marzo de 2024, Lord Peña también reveló al menos tres vulnerabilidades en el sitio web del Servicio de Administración Tributaria (SAT) justo en medio de la campaña para la declaración anual de impuestos de personas físicas para el año 2023. Además, el pasado domingo 31 de marzo, publicó en Breach Forums la oferta de acceso a los servidores internos del Órgano de Fiscalización Superior del estado de Veracruz (ORFIS) por tan solo 1,500 dólares, equivalente a aproximadamente $24,981 MXN.

En cada uno de los casos mencionados, el hacker proporcionó pruebas de acceso a la información al publicar capturas de pantalla que exhibían datos confidenciales no disponibles para el público en general y ofreció negociar a través de su cuenta de *Telegram*.

¿Qué hay del hackeo al gobierno de la Ciudad de México?

Publimetro confirmó que el servidor Zimbra, utilizado por varias entidades gubernamentales de la Ciudad de México, fue efectivamente comprometido. De los 1.4 terabytes descargados por *Lord Peña*, al menos 415 gigabytes fueron enviados a este medio de comunicación, lo que equivale a cientos de miles de correos electrónicos.

Según una primera revisión, de las 2,300 cuentas de correo electrónico a las que accedió el ciberatacante, se filtraron a este medio los datos de 1,327. Estos datos incluyen conversaciones sobre protocolos durante la pandemia de Covid-19, así como información relacionada con la autorización de obras en la capital, presupuestos, entre otros temas que aún no han sido revisados por la amplitud de la información.

La base de datos de correos abarca todos los mensajes recibidos y enviados por funcionarios de diversas entidades, como el Museo de Arte Popular, la Procuraduría Social, la Secretaría de Obras y Servicios, centros del DIF, el Consejo de Evaluación de la Ciudad de México, así como las secretarías de Finanzas, Medio Ambiente, Educación, Ciencia, Tecnología e Innovación, y las 16 alcaldías de la CDMX, entre otras dependencias del gobierno local.

"De manera similar a lo ocurrido con la UNAM, el acceso fue a través de una vulnerabilidad pública en Zimbra, específicamente la CVE-2019-9670. Dado que esta vulnerabilidad es ampliamente conocida, ya existían alojadas web shells. Para mitigar esta vulnerabilidad, implementé una solución provisional que consistió en modificar los permisos del sistema, evitando así la subida de nuevas web shells", explicó *Lord Peña* a *Publimetro*.

Para obtener más detalles sobre el alcance del ataque, se consultó al hacker si su acceso se limitaba únicamente a la información o si tenía control total sobre las cuentas. Su respuesta fue la siguiente: "Sí, tengo acceso total. Como es mucha información, apenas la estoy analizando".

El hacker también otorgó acceso a ciertas cuentas a otros miembros del grupo Mexican Mafia, donde operan otros atacantes que han divulgado sus intrusiones de varias dependencias gubernamentales. Entre ellos se encuentran *Pancho Villa*, líder del grupo, quien hackeó la Secretaría de Seguridad y Protección Ciudadana de Oaxaca, y *Buda*, quien el pasado 31 de marzo puso a la venta en foros una base de datos con subdominios del gobierno del Estado de México.

No se aprendió de los Guacamaya Leaks

En entrevista con *Publimetro*, el especialista y fundador de la firma de ciberseguridad SILIKN, Víctor Ruiz, destacó el gobierno, en sus diferentes niveles, no ha optimizado sus sistemas de seguridad, a pesar de que las vulnerabilidades de Zimbra se hicieron evidentes en el país después del hackeo que realizó el grupo Guacamaya al servidor de la Secretaría de la Defensa Nacional (Sedena).

"Muchas dependencias siguen utilizando Zimbra y no se han encargado de corregir la vulnerabilidad. Se encuentran vulnerabilidades a cada rato y no lo dan a conocer. (...) No se trata de 'pobre gobierno', son nuestros datos de empleo, de salud, económicos (...) Me da la impresión de que no invierten en ciberseguridad y, en esta última parte del sexenio, pudieran tomarlo como pretexto de pérdida de información a raíz de presuntos hackeos", advirtió Ruiz.

Asimismo, de acuerdo con una investigación de SILIKN, entre las dependencias que podrían ser afectadas bajo la misma vulnerabilidad se encuentran: Secretaría de Desarrollo Económico de la Ciudad de México, Portal de Transparencia de la Ciudad de México, Secretaría de la Función Pública, gobierno del estado de Durango, Secretaría de Educación de Veracruz; Servicio Nacional de Sanidad, Inocuidad y Calidad Agroalimentaria; Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, Secretaría de Seguridad y Protección Ciudadana, Gobierno del Estado de Oaxaca, Secretaría de Salud, Secretaría de Educación del estado de Puebla, gobierno del estado de Tabasco, Secretaría de Educación Pública, Suprema Corte de Justicia de la Nación, gobierno del estado de Guanajuato, Secretaría del Trabajo y Previsión Social, gobierno del estado de Nuevo León, gobierno del Estado de México, Secretaría de Salud de Veracruz, Poder Judicial del estado de Nuevo León, Instituto Mexicano de la Juventud, Secretaría de Seguridad Pública de Puebla, Secretaría de Educación de Coahuila, Instituto Nacional de Investigaciones Forestales, Agrícolas y Pecuarias, así como la Secretaría de Finanzas de la Ciudad de México.

Evidencias. Diversas capturas de pantalla fueron reveladas como prueba del hackeo. / CAPTURA DE PANTALLA

CIFRAS

1.4

terabytes de información.

2,300

cuentas de correo vulneradas.

2.1

millones de correos filtrados.

"Nos deben una respuesta de qué están haciendo y que lo reconozcan, no está mal reconocer las vulnerabilidades"

Víctor Ruiz
Especialista y fundador de la firma de ciberseguridad SILIKN