Hackers vulneran dos secretarías de Puebla

#GUACAMAYA LEAKS

Hackers vulneran dos secretarías de Puebla

DANIEL CRUZ
El Sol de Puebla

El Centro de Operaciones del Ciberespacio de la Sedena alertó en abril pasado sobre el hackeo

PUEBLA. Las barreras de seguridad informática del Gobierno de Puebla fueron derribadas en un ataque informático que sufrieron los servidores de la Secretaría de la Función Pública (SFP) y de la Secretaría de Educación Pública (SEP), según alertaron en abril pasado agentes de inteligencia militar, lo que dejó vulnerables casi media centena de cuentas de correos electrónicos institucionales.

En abril pasado, personal del Centro de Operaciones del Ciberespacio (COC) de la Secretaría de la Defensa Nacional (Sedena), así como del brazo institucional de la Organización de los Estados Americanos (OEA) para la detección de amenazas informáticas, ubicaron que, a nivel mundial, quedaron expuestas las credenciales de acceso de un total de un millón 753 mil 658 cuentas gubernamentales, incluidas 44 de la SFP y la SEP del gobierno poblano.

El reporte, enviado a través de un correo confidencial el 22 de ese mismo mes, es parte de los archivos de la Sedena hechos públicos por el grupo de activistas informáticos Guacamaya, en poder de **El Sol de Puebla.**

La dependencia más afectada por este ataque virtual fue la SFP, encabezada por Juan Carlos Moreno Valle Abdala. Los piratas informáticos atacaron los subdominios de la dependencia en los que los funcionarios rinden sus declaraciones patrimoniales, Declaranet.

De acuerdo con agentes del COC, un total de 29 cuentas de correo electrónico asociadas al sistema Declaranet fueron comprometidas por ese ataque.

El resto de cuentas afectadas pertenecen a la SEP, cuyo titular en ese entonces era Melitón Lozano Pérez. En este caso, el blanco de los atacantes fue el subdominio que alberga el Sistema de Control Escolar del estado de Puebla (SICEP) pues la intromisión alcanzó a vulnerar 15 perfiles de ese subdominio. Pese a que fue en abril pasado cuando personal de la Sedena detectó la intrusión, en el cuerpo del informe no se indicó cuándo fue que ocurrieron dichas filtraciones. Lo que sí se supo fue que las mismas pudieron concretarse gracias al malware conocido como Stealer.

De acuerdo con la compañía mundial de desarrolladores de antivirus Avast, este

tipo de amenazas catalogadas como troyanos pueden infectar de forma casi inmediata a los usuarios que comparten una misma red. Aunque los piratas informáticos poseen un amplio abanico de opciones para infiltrar usuarios algunas de las más comunes son a través de redes sociales o videojuegos.

Para infiltrar sistemas, los hackers utilizan técnicas de anzuelo, como el ofrecimiento de supuestos contenidos gratuitos: aplicaciones, juegos, imágenes, música, etcétera. Esto provoca que, para la obtención de estos regalos, se pida a los usuarios registrarse con el correo electrónico y contraseña. Así se genera la intromisión de servidores, en este caso, de subdominios.

De acuerdo con la empresa de seguridad digital Kaspersky, México es la décimo cuarta nación a nivel mundial más atacada por piratas informáticos, siendo los virus de tipo troyano, similares a los que se entrometieron en los servidores del Gobierno estatal, los más comunes.

El Sol de México publicó que la Auditoría Superior de la Federación (ASF) advirtió, desde 2020, que la ciberseguridad de la Sedena era deficiente, y alertó así sobre un posible compromiso de información similar al que enfrentó la dependencia federal en meses pasados.

29

CUENTAS de correo electrónico asociadas al sistema Declaranet fueron comprometidas

15

PERFILES vulneró la intromisión en el Sistema de Control Escolar del estado de Puebla

Las filtraciones pudieron concretarse gracias al malware conocido como Stealer

A nivel mundial, quedaron expuestas las credenciales de acceso de un millón 753 mil 658 cuentas gubernamentales, incluidas 44 de la SFP y la SEP del gobierno poblano