Ciberataque a Pemex, alerta para las grandes empresas

A través de un comunicado de prensa emitido el domingo 10 de noviembre, Pemex informó haber sufrido "intentos de **ataques cibernéticos**" que de acuerdo con la compañía, **solo afectaron el cinco por ciento de las computadoras**, sin que el incidente afectara sus operaciones.
Para el investigador de seguridad de ESET Latinoamérica, Miguel Ángel Mendoza, **aparentemente se trata de un ataque dirigido, que debe servir como señal de alerta para otras compañías,** sobre todo teniendo en cuenta lo que sucedió recientemente en España con los dos **ataques de ransomware que afectaron a la consultora IT Everis** y a una de las principales cadenas de radio de aquel país, como es Cadena SER.
Existen códigos maliciosos, como **Emotet** o **Trickbot**, que son utilizados para propagar diferentes tipos de amenazas; es decir, funcionan como downloaders que también distribuyen ransomware, explica Mendoza.

"En este tipo de ataques dirigidos, una vez que se compromete un equipo, se utilizan herramientas para realizar movimientos laterales dentro de las redes corporativas, tal es el caso de Empire (basado en PowerShell), una herramienta utilizada por atacantes para estos propósitos. Otras **campañas de propagación de ransomware en ataques dirigidos se basan en la explotación de vulnerabilidades, como es el caso de BlueKeep**", agrega el especialista.

Recomendaciones

Frente a este escenario, Mendoza recuerda algunas de las principales recomendaciones dirigidas a empresa y usuarios para estar protegidos ante una amenaza de esta naturaleza:

· **Utilizar una solución antimalware** actualizada y correctamente configurada.
· **Actualizar los sistemas operativos y software** en general, para corregir vulnerabilidades conocidas.
· **Evitar acceder a enlaces o descargar archivos** adjuntos de correos electrónicos sospechosos.
· **Realizar respaldos de información** de manera periódica, de acuerdo con la criticidad de los datos en cuestión.
· **Evitar realizar el pago del rescate**, ya que esto no garantiza la obtención de las claves de descifrado, y en caso de obtenerlas, las mismas no son funcionales. Además, con el pago del rescate se financia la industria cibercriminal.
· **Educar y concientizar a los miembros de la organización** en materia de seguridad, para evitar que se conviertan en la puerta de acceso para las amenazas de este estilo.