LITORALPRESS

Fecha: 10-08-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo C
Tipo: Noticia general
Título: **Cámara de Diputados bajo asedio: 21 millones de intentos de acceso a la red**

Pág. : 4
Cm2: 300,5

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Parte de las cifras sobre ciberseguridad corresponden solamente a julio

Cámara de Diputados bajo asedio: 21 millones de intentos de acceso a la red

De calificar de "alto riesgo" una comisión investigadora, ahora la corporación reveló las amenazas informáticas a las que han debido hacer frente sus sistemas.

RIENZI FRANCO

Si días atrás fue llamativo el que Seguridad de la Cámara declarara de "alto riesgo" la comisión investigadora por la esquiva reconstrucción de casas en Viña del Mar producto del incendio de febrero del año pasado, ahora al parecer la Cámara de Diputados estaría bajo un asedio informático. De ello se dio cuenta de manera pública en la corporación.

Solo durante el mes de julio, el sistema bloqueó 2 millones de correos electrónicos maliciosos. El Departamento de Informática de la Cámara suele desarrollar herramientas propias en lo legislativo y aplicaciones incluso sobre IA; asomaron con los aplicativos antes de la pandemia y durante el covid la necesidad de las tareas a distancia las profundizó.

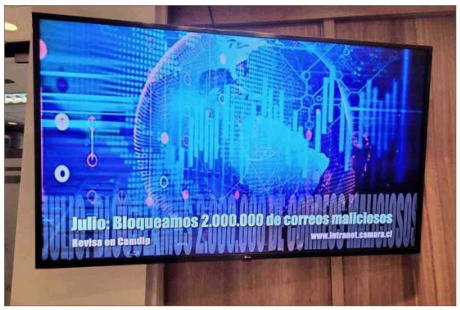
De ahí se originan los bloqueos ante amenazas en la red, a cargo del equipo de ciberseguridad. Los riesgos detectados se refieren a 21.955.609 de intentos de acceso perimetral a la red analizados; 2 millones de correos *spam* o maliciosos bloqueados; 177 eventos de *malware* bloqueados y 5.400.000 páginas de "contenido inapropiado" bloqueadas".

Así como se da cuenta de la incidencia informática, también se entregan recomendaciones a los usuarios de la Cámara, apelando a su "rol clave" en "seguir buenas prácticas", como "no hacer clic en enlaces sospechosos", usar contraseñas robustas y únicas", bloquear tu equipo al ausentarte" y "reportar actividades inusuales de inmediato al equipo de TI".

También se informa a la comunidad de usuarios acerca de las formas en que los atacantes de los sistemas actúan. Lo hacen, afirman, a través de la "ingeniería social", que definen como "una técnica de manipulación para engañar a las personas y así obtener acceso a información, sistemas o ejecutar acciones críticas dentro de una organización".

De cómo actúan los delincuentes informáticos, se indica que "se hacen pasar por figuras conocidas o confiables, como funcionarios de áreas internas, proveedores de servicios externos, autoridades públicas o jefaturas, instituciones como bancos o servicios del Estado y utilizan excusas como 'necesitamos validar tu clave institucional', 'se detectó una actividad irregular en tu cuenta' o 'adjuntamos una factura pendiente de pago del Congreso'".

Estos ataques, prosigue el informativo, se plasman mediante correos falsos (*phishing*), llamadas telefónicas (vishing) o por mensajes personalizados (*spear phishing*). Estos antecedentes son parte de las paletas informativas internas de la Cámara, disponibles en pantallas y en los tradicionales ficheros colgados en las paredes de los pasillos con alto tránsito de funcionarios.



En pantallas informativas de la Cámara se dieron a conocer parte de las amenazas recibidas durante el mes pasado.