

Fecha: 17-01-2026
 Medio: El Longino
 Supl. : El Longino
 Tipo: Columnas de Opinión
 Título: **Columnas de Opinión: Cuando el navegador te espía: la amenaza silenciosa detrás de las extensiones**

Pág. : 9
 Cm2: 302,6

Tiraje: 3.600
 Lectoría: 10.800
 Favorabilidad: No Definida



**Edgardo Fuentes Cáceres - Director
Ingeniería en Ciberseguridad UNAB**

Las extensiones de navegador son pequeños programas que se instalan en plataformas como Chrome, Edge o Firefox para añadir funciones específicas: bloquear publicidad, traducir textos, gestionar contraseñas, grabar reuniones o personalizar la experiencia de navegación. Una vez integradas, operan de manera permanente en segundo plano, con acceso directo a los sitios que visitamos, al contenido que visualizamos e incluso a los datos que ingresamos. Esa cercanía técnica, que las hace tan útiles, es también lo que las convierte en un objetivo privilegiado para el abuso.

El caso DarkSpectre expone una de las paradojas más incómodas

Cuando el navegador te espía: la amenaza silenciosa detrás de las extensiones

de la seguridad digital: cuanto más cotidiano y útil parece un recurso tecnológico, mayor es nuestra disposición a confiar en él sin cuestionamientos. Millones de usuarios instalaron extensiones que prometían funciones simples como mejorar la navegación, facilitar reuniones online o personalizar pestañas, sin sospechar que, tras esa aparente normalidad, se gestaba una de las campañas de malware más silenciosas y masivas de los últimos años. La operación no se caracterizó por ataques ruidosos ni por fuerza bruta, sino por paciencia estratégica. Las extensiones funcionaron durante largos períodos sin comportamientos sospechosos, acumulando descargas, buenas evaluaciones y legitimidad dentro de las tiendas oficiales. Ese tiempo de "conducta limpia" fue clave: generó confianza tanto en los usuarios como en los mecanismos de revisión de plataformas como Chrome Web Store o Firefox Add-ons.

Cuando el malware se desplegó, lo hizo de forma selectiva y progresiva. No todos los usuarios fueron afectados

al mismo tiempo ni de la misma manera, lo que dificultó enormemente la detección. Además, se emplearon técnicas poco convencionales, como la carga de código oculto en archivos aparentemente inofensivos y la comunicación directa con servidores externos que permitía modificar el comportamiento de la extensión sin pasar por nuevas revisiones. En la práctica, el navegador -una de las herramientas más usadas para trabajar, estudiar y comunicarse- se transformó en un punto de observación permanente. Este tipo de ataques demuestra que la vulnerabilidad no reside solo en el software, sino en el modelo de confianza que hemos construido alrededor de él. Asumimos que, por estar disponible en una tienda oficial, una extensión es segura de forma indefinida. Sin embargo, las revisiones suelen ser iniciales y automáticas, incapaces de detectar cambios posteriores en el código. El resultado es un ecosistema donde una herramienta legítima puede convertirse, con el tiempo, en un vector de espionaje, robo de datos o fraude. La principal enseñanza es clara: la seguridad del navegador

debe ser tratada con el mismo nivel de atención que cualquier otro sistema crítico. Las extensiones poseen permisos amplios: pueden leer lo que escribimos, ver lo que navegamos e incluso interactuar con sesiones de trabajo o reuniones. Minimizar ese riesgo es una responsabilidad compartida entre plataformas, desarrolladores y usuarios.

Algunas prácticas básicas pueden marcar una diferencia real: instalar solo extensiones estrictamente necesarias y eliminar las que no se usan; revisar con atención los permisos solicitados, especialmente cuando una función simple pide acceso total a todos los sitios web; desconfiar de extensiones genéricas, con desarrolladores poco claros o nombres demasiado similares a herramientas populares; mantener el navegador actualizado y revisar periódicamente el listado de extensiones activas; y, en entornos laborales o educativos, aplicar políticas que limiten qué extensiones pueden instalarse.

DarkSpectre no fue un accidente ni una anomalía, sino una advertencia. Nos recuerda que la amenaza más efectiva no siempre es la más visible, sino aquella que se integra sin fricción en nuestra rutina digital. En un escenario donde el navegador se ha convertido en oficina, aula y espacio personal, cuestionar lo que instalamos ya no es paranoia: es una forma básica de higiene digital.

Los columnistas expresan opiniones absolutamente personales y no representan necesariamente la línea editorial Longino de Iquique.

Ambulancia: 131	57 2491517 / 57-2493025
Bomberos: 132	Cuerpo de Bomberos de Alto Hospicio: 57 2499390
Carabineros: 133	Aguas del Altiplano: 600 600 9900
Rescate Marítimo: 137	Eliqa: 600 600 2233
Cuerpo de Bomberos de Santa Rosa de Huantajaya:	Emergencia Alto Hospicio: 57 2583050

Teléfonos Emergencias Alto Hospicio

Diario El Longino debe su nombre a un merecido homenaje al legendario Tren Longitudinal Norte que corrió entre Iquique y La Calera desde 1929 hasta 1975 fecha en que, por una nefasta decisión gubernamental, dejó de transportar a miles de chilenos.

Director	Domicilio
Adolfo Vargas Jofré	San Martin 428/ Of 2.
Correo	Departamento Comercial adolfovargas@diariolongino.cl
Representante Legal	Patricio Felix Meza Flores Cel: +56 9 61201918
Email	Patricio Felix Meza Flores E.I.R.L contacto@diariolongino.cl Fono +56 9 61201918

El Longino