Una vulnerabilidad de seguridad, que ya ha sido corregida en el navegador Opera, podría haber permitido a una extensión maliciosa acceder de forma no autorizada y completa a las API privadas.

El ataque, llamado CrossBarking, habría permitido realizar acciones como capturas de pantalla, ajustes en la configuración del navegador y toma de control de cuentas, según informó Guardio Labs.

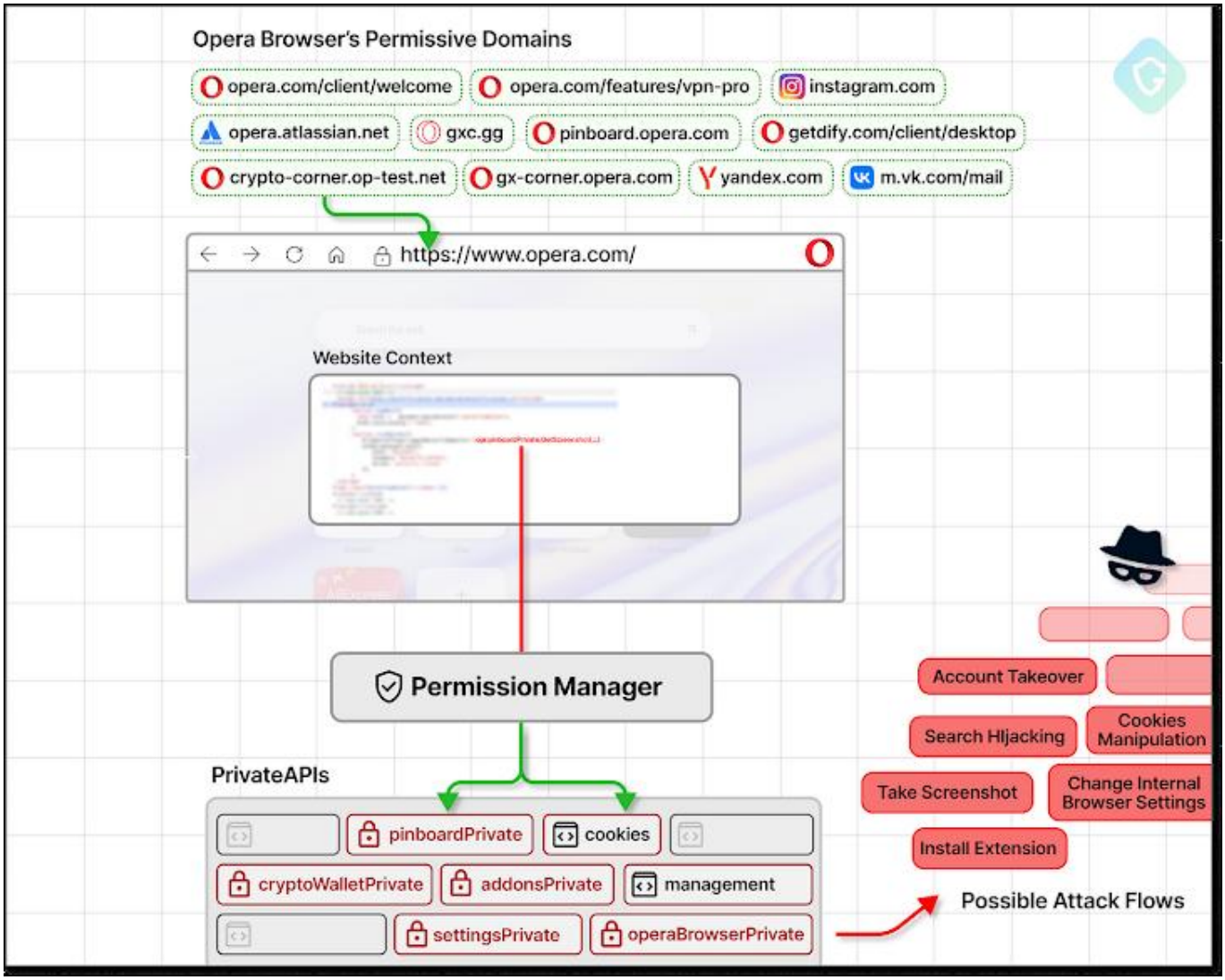
Para demostrar la falla, la compañía publicó una extensión aparentemente inocua en la Chrome Web Store, la cual podía aprovechar esta vulnerabilidad al instalarse en Opera, generando un ataque *«entre tiendas de navegadores».*

> *«Este caso no solo muestra el conflicto constante entre productividad y seguridad, sino que también revela un interesante vistazo a las técnicas que utilizan los actores de amenazas actuales, que operan casi sin ser detectados»,* comentó Nati Tal, jefe de Guardio Labs, en un informe.

Opera abordó el problema el 24 de septiembre de 2024 tras una divulgación responsable. Sin embargo, esta no es la primera vez que se detectan problemas de seguridad en el navegador.

En enero de este año, surgieron detalles sobre una vulnerabilidad conocida como MyFlaw, que explota una función legítima llamada My Flow para ejecutar cualquier archivo en el sistema operativo.

Este último método de ataque se basa en que varios subdominios públicos de Opera tienen acceso privilegiado a las API privadas del navegador. Estos dominios se utilizan para características específicas de Opera, como Opera Wallet y Pinboard, así como para el desarrollo interno.



Algunos de estos dominios, que también incluyen sitios de terceros, se listan a continuación:

- crypto-corner.op-test.net
- op-test.net
- gxc.gg
- opera.atlassian.net
- pinboard.opera.com
- instagram.com

- yandex.com

Aunque el aislamiento sandbox asegura que el contexto del navegador permanezca separado del sistema operativo, la investigación de Guardio reveló que los scripts de contenido en una extensión podrían inyectar JavaScript malicioso en estos dominios con permisos excesivos y acceder a las API privadas.

Aquí tienes el texto reescrito con un lenguaje diferente pero conservando el mismo significado:

> *«El script de contenido sí tiene acceso al DOM (Modelo de Objetos del Documento). Esto le permite modificarlo de forma dinámica, especialmente añadiendo nuevos elementos»,* señaló Tal.

Con este acceso, un atacante podría capturar pantallas de todas las pestañas abiertas, extraer cookies de sesión para tomar control de cuentas e incluso alterar la configuración de DNS sobre HTTPS (DoH) del navegador para resolver dominios a través de un servidor DNS que el atacante controle.

Esto puede permitir ataques de intermediario (AitM) muy efectivos, redirigiendo a las víctimas a versiones maliciosas cuando intentan acceder a sitios de bancos o redes sociales.

La extensión maliciosa podría publicarse como algo inofensivo en cualquiera de los catálogos de complementos, incluido el Chrome Web Store de Google. Desde allí, los usuarios podrían descargarla e instalarla en sus navegadores, desencadenando el ataque. Sin embargo, se requiere permiso para ejecutar JavaScript en cualquier sitio web, especialmente en los dominios con acceso a las API privadas.

Dado que extensiones de navegador maliciosas logran infiltrarse repetidamente en las tiendas oficiales y que algunas legítimas no son transparentes en sus prácticas de recopilación de datos, estos hallazgos destacan la importancia de ser cautelosos antes de

instalarlas.

> *«Las extensiones de navegador tienen un poder considerable, tanto para bien como para mal. Por eso, es fundamental que las políticas de control las supervisen de forma rigurosa»,* comentó Tal.
>
> *«El modelo de revisión actual es insuficiente; recomendamos reforzarlo con más personal y métodos de análisis constantes que monitoricen la actividad de una extensión incluso después de su aprobación. También es crucial que se exija una verificación de identidad real para las cuentas de desarrolladores, de modo que no baste con usar un correo electrónico gratuito y una tarjeta prepaga para registrarse.»*