En una nueva técnica de phishing, se demostró que se puede abusar de la función Modo de Aplicación en los navegadores web basados en Chromium para *«crear aplicaciones de phishing de escritorio realistas».*

El modo de aplicación está diseñado para ofrecer experiencias similares a las nativas de una forma que hace que el sitio web se inicie en una ventana de navegador separada, al mismo tiempo que muestra el ícono de favoritos del sitio web y oculta la barra de direcciones.

Según el investigador de seguridad mr.d0x, quien también ideó el método de ataque del navegador en el navegador (BitB) a inicios de 2022, un hacker puede aprovechar este comportamiento para recurrir a algunos trucos de HTML/CSS y mostrar una barra de direcciones falsa en la parte superior de la ventana y engañar a los usuarios para que revelen sus credenciales en formularios de inicio de sesión no autorizados.

> *«Aunque esta técnica está destinada más al phishing interno, técnicamente aún puede usarla en un escenario de phishing externo. Puede entregar estas aplicaciones falsas de forma independiente como archivos»,* dijo mr.d0x.

Esto se logra configurando una página de phishing con una barra de dirección falsa en la parte superior y configurando el parámetro -app para apuntar al sitio de phishing que aloja la página.

Además, el sitio de phishing controlado por el atacante puede usar JavaScript para realizar más acciones, como cerrar la ventana inmediatamente después de que el usuario ingrese las credenciales o cambiar su tamaño y posicionamiento para lograr el efecto deseado.

Cabe mencionar que el mecanismo funciona en otros sistemas operativos como macOS y Linux, lo que lo convierte en una posible amenaza multiplataforma. Sin embargo, el éxito del ataque se basa en el hecho de que el atacante ya tiene acceso a la máquina del objetivo.

Debido a esto, Google está eliminando gradualmente la compatibilidad con las aplicaciones

de Chrome en favor de las aplicaciones web progresivas (PWA) y las tecnologías estándar de la web, y se espera que la función se suspenda completamente en Chrome 109 o posterior en Windows, macOS y Linux.

En una declaración, la compañía dijo que *«la fucnión –app quedó obsoleta antes de que se publicara esta investigación, y estamos teniendo en cuenta su potencial de abuso al considerar su futuro»*.

> *«Los usuarios deben ser conscientes de que ejecutar cualquier archivo proporcionado por un atacante es peligroso. La navegación segura de Google ayuda a proteger contra archivos y sitios web no seguros. Aunque la navegación segura está habilitada predeterminadamente en Chrome, los usuarios pueden querer habilitar la protección mejorada, que inspecciona la seguridad de las descargas para advertir mejor cuando un archivo pueda ser peligroso».*

Los hallazgos se producen cuando las investigaciones de Trustwave SpiderLabs muestran que los ataques de contrabando de HTML son una ocurrencia común, con archivos .HTML (11.39%) y .HTM (2.7&) que representan el segundo tipo de archivo adjunto más enviado como spam después de las imágenes .JPG (25.29%).