Una nueva técnica de phishing llamada ataque de navegador en el navegador (BitB) se puede explotar para simular una ventana de navegador dentro del navegador web para falsificar un dominio legítimo, lo que hace posible realizar ataques de phishing más convincentes.

Según el probador de penetración e investigador de seguridad, con alias mrd0x_, el método aprovecha las opciones de inicio de sesión único (SSO) de terceros integradas en sitios web como *«Iniciar Sesión con Google»* u otras plataformas.

Aunque el comportamiento predeterminado cuando un usuario intenta iniciar sesión a través de estos métodos recibe una ventana emergente para completar el proceso de autenticación, el ataque BitB tiene como objetivo replicar todo este proceso utilizando una combinación de código HTML y CSS para crear una ventana del navegador completamente fabricada.

> *«Combiné el diseño de la ventana con un iframe que apunta al servidor malicioso que aloja la página de phishing, y es básicamente indistinguible». JavaScript se puede usar fácilmente para hacer que la ventana aparezca en un enlace o en un clic de botón, en la carga de la página, etc,»,* dijo mrd0x_.

Aunque este método facilita significativamente el montaje de campañas de ingeniería social efectivas, cabe mencionar que las víctimas potenciales deben ser redirigidas a un dominio de phishing que puede mostrar una ventana de autenticación falsa para la recolección de credenciales.

> *«Pero una vez que llega al sitio web propiedad del atacante, el usuario estará tranquilo mientras escribe sus credenciales en lo que parece ser el sitio web legítimo (porque la URL confiable lo dice)»,* agregó mrd0x_.