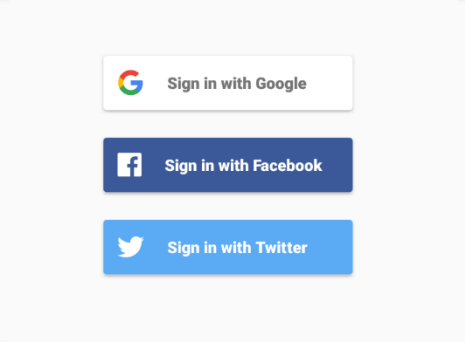
CUIDADO: Browser In The Browser (BITB), la nueva técnica que dificulta identificar un phishing.

Una de las técnicas más utilizadas por los ciberdelincuentes es el phishing, la que busca engañar a sus víctimas con correos o páginas web falsas, con el objetivo de inyectar programas maliciosos u obtener los datos personales de los usuarios, como claves bancarias o de redes sociales y así robarles dinero o suplantarlos en internet, entre otros delitos.

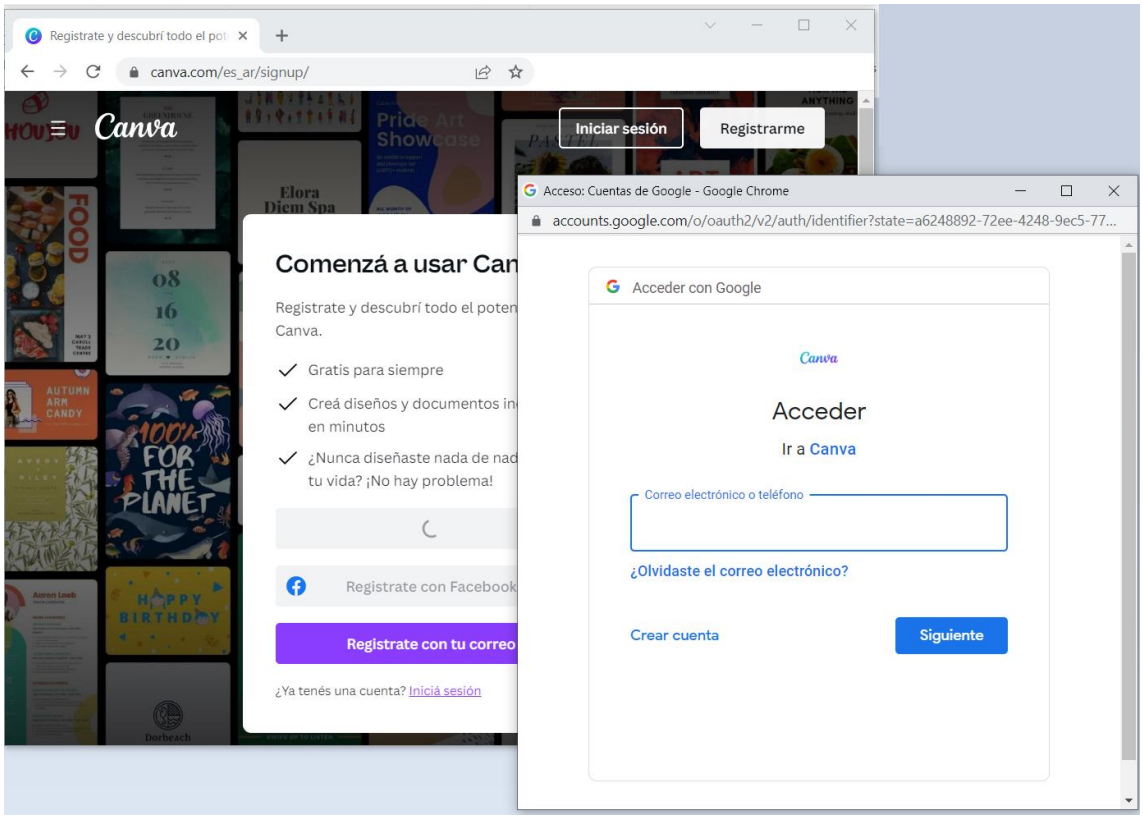
Y así como los sistemas de ciberseguridad han ido mejorando, las técnicas de phishing también han evolucionado. Un ejemplo de esto es la técnica conocida como Browser in the Browser (BITB).

Anunciada a un público masivo recién en marzo de este año, por el investigador de ciberseguridad identificado como mrd0x, es una nueva forma de explotar las **opciones de inicio de sesión único (SSO)** existentes en algunos sitios web.



Así, esta nueva forma de phishing imita las ventanas pop up que se despliegan en todo tipo de sitios hoy por hoy, entregando la opción de iniciar sesión usando las credenciales de Google, Facebook, Twitter u otra plataforma, una opción popular ya que es más cómoda para el usuario y le exige recordar menos contraseñas.

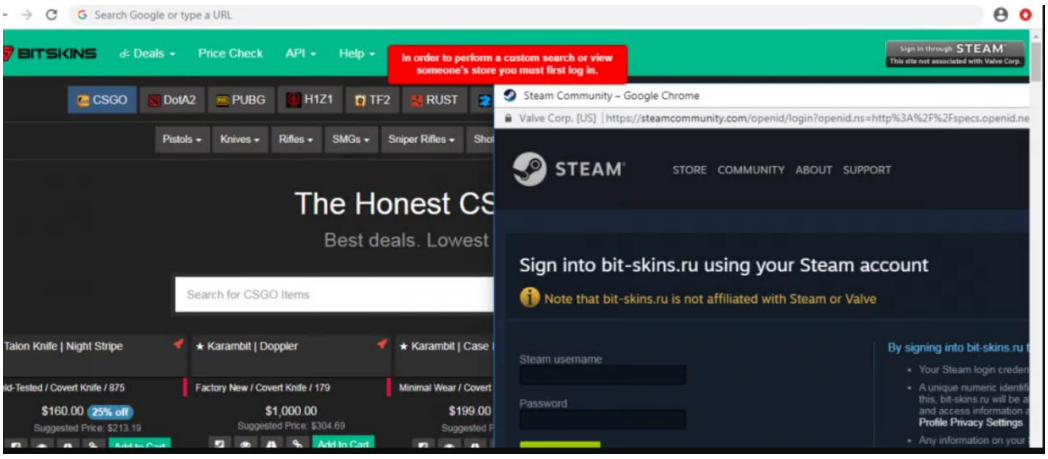
Por ejemplo, en Canva, para iniciar sesión con Google se despliega la siguiente ventana, totalmente legítima:



Esta nueva forma de phishing imita esos pop ups legítimos de inicio de sesión único, mostrando a la víctima lo que parece un pop up real, pero es un formulario falso para robar sus contraseñas. Para desplegarse, eso sí, necesita que el usuario haga clic en una página web comprometida previamente por los ciberdelincuentes.

En esta web comprometida se usa una combinación de código HTML, CSS y JavaScript para crear la ventana fraudulenta y que esta muestre una URL (la dirección de la página web) que aparente ser la dirección verdadera, lo cual dificulta la identificación del phishing. **Este es un gran riesgo, ya que usualmente chequear la URL es una de las formas en que podemos protegernos para distinguir si estamos en un sitio real o en uno fraudulento**.

Aunque Browser In The Browser se dio a conocer más ampliamente en marzo, ya en febrero el equipo de Zscaler ThreatLabZ denunció el uso de esta técnica para simular el inicio de sesión en la plataforma Steam, una de las páginas de videojuegos más populares.



A lo anterior, se suma la alerta en marzo del Grupo de Análisis de Amenazas (TAG, de su sigla en inglés) de Google, quienes indicaron que los hackers bielorrusos de Ghostwriter, estaban utilizando también esta técnica.

Recomendaciones:

Ante la posibilidad de que esta técnica sea cada vez más utilizada, las recomendaciones son las siguientes:

- Intentar arrastrar la ventana emergente hasta el borde del navegador es una manera de detectar un ataque BITB. Si no puede salir del navegador, entonces no es una ventana real.
- No abrir correos ni mensajes (ya sea SMS, WhatsApp, Facebook Messenger o cualquier app que tenga mensajería) de dudosa procedencia.
- No hacer clic de enlaces y archivos recibidos en apps de mensajería o email. Siempre es mejor ingresar a bancos e instituciones a través de escribir su URL directamente en la barra de direcciones.
- Si parece ser un mensaje importante, llamar directamente a la institución para aclarar la situación. Lo mismo cuando se recibe un enlace sospechoso de un amigo o contacto de redes sociales.
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por Internet.