BOLETÍN DE ALERTA

Boletín Nro.: 2022-22
Fecha de publicación: 29/04/2022
Tema: Nuevo método de phishing Browser in the Browser (BITB)

Descripción:

Se ha descubierto una técnica novedosa de phishing que permitiría a un atacante, ejecutar dicho ataque aprovechando las opciones de inicio de sesión único (*SSO*) integradas en diferentes sitios web.

El método denominado Browser in the Browser (BITB) utiliza plantillas prefabricadas para crear ventanas emergentes (*frames*) falsas en Google Chrome, pero muy realistas, que incluyen direcciones URL y títulos personalizados que pueden utilizarse para que los ataques de phishing sean más efectivos.

El novedoso método aprovecha las opciones de inicio de sesión único (*SSO*) de terceros integradas en sitios web que emiten ventanas emergentes para la autenticación, como "*Iniciar sesión con Google*", *Facebook*, *Apple* o *Microsoft*. Si bien, el comportamiento predeterminado cuando un usuario intenta iniciar sesión a través de estos métodos es recibir 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.

Actualmente existen plantillas para ejecutar dicho ataque Browser in the Browser (BITB) en Internet (GitHub).

Impacto:

La explotación de este método permitiría a un atacante replicar una ventana emergente similar a la que se visualiza al iniciar sesión (SSO), logrando de esta forma a partir del pop-up de inicio de sesión ilegítimo, robar las credenciales.

Detección:

Para comprobar si el formulario de acceso que aparece en tu pantalla es falso, sigue los siguientes pasos:

- Minimizar la ventana del navegador desde que apareció el formulario. Si el formulario de acceso que se supone que está en una ventana separada también desaparece, entonces es falso. Las ventanas reales permanecen siempre en la pantalla en primer plano.

- Intentar mover la ventana de inicio de sesión más allá del borde de la ventana principal. Una ventana real cruzará fácilmente, una falsa se quedará atascada.

Adicionalmente, se sugiere para la detección de dicho método utilizar una extensión para el navegador, proporcionada en el siguiente enlace:

- https://github.com/odacavo/enhanced-iframe-protection

Mitigación:

Para los usuarios en general se recomienda activar el doble factor de autenticación (2FA) para el acceso a cuentas (en caso de ser posible).

Además para los equipos de desarrollado se recomienda tener en cuenta los siguientes puntos:

1. Analizar visualmente la URL es insuficiente dado que la URL visible justamente fue modificada por el atacante para que sea idéntica a la URL verdadera, por lo que diferenciarlas sería muy difícil. Realizar campañas de concienciación (CISA - mejores prácticas de seguridad de correos electrónicos falsos y mensajes sospechosos) para explicar esta nueva técnica a los usuarios finales.
2. Enviar las cabeceras de respuesta apropiadas a X-Frame-Options de *HTTP* que fuerce al navegador para evitar ataques de *click-jacking* y no permita enmarcar otros dominios.
3. Utilizar políticas de seguridad de contenido (CSP) en las cabeceras como mecanismo adicional de detección y prevención de *clickjacking*.
4. Implementar mejores prácticas de desarrollo para evitar Clickjacking y así garantizar que el marco actual es la ventana de más alto nivel.

Información adicional:

- https://mrd0x.com/browser-in-the-browser-phishing-attack/
- https://blog.segu-info.com.ar/2022/03/templates-de-phishing-browser-in-browser.html
- https://github.com/mrd0x/BITB
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bfd-dos-wGQXrzxn
- https://www.cert.gov.py/noticias/nuevo-metodo-de-phishing-browser-browser-bitb
- https://portswigger.net/web-security/clickjacking