# RASTREO Y FUNCIONAMIENTO DEL BROWSER HIJACKER “SEARCHBOX”

## Introducción a la ciberseguridad

En la actualidad, la ciberseguridad se ha convertido en un tema de vital importancia en el entorno digital. Con la constante evolución de las amenazas, es esencial que las organizaciones implementen estrategias proactivas para fortalecer su resiliencia y proteger su información. El MITRE ATT&CK Framework ofrece un conjunto de mitigaciones que actúan como barreras estratégicas contra posibles ataques de Browser hijacker. Estas medidas abarcan desde la gestión de cuentas hasta la prevención de comportamientos maliciosos en los endpoints, y son fundamentales para protegerse contra las amenazas digitales en constante evolución.

## Definición y funcionamiento

Un Browser hijacker es un tipo de software malicioso que altera la configuración del navegador web de un usuario sin su consentimiento. Su objetivo principal es redirigir el tráfico web hacia sitios específicos, con el fin de generar ingresos publicitarios o promover contenido no deseado. Esto puede afectar negativamente la experiencia de navegación del usuario y comprometer su privacidad y seguridad en línea. El funcionamiento de un Browser hijacker incluye la modificación de la página de inicio, el motor de búsqueda predeterminado y otras configuraciones del navegador, así como la recopilación de datos sensibles del usuario. Es importante tomar medidas inmediatas para eliminar este tipo de software y protegerse contra sus amenazas.

## Impacto en la Seguridad del Sistema

El secuestrador de navegador Searchbox puede tener un impacto significativo en la seguridad del sistema de los usuarios y los sistemas afectados. Una de las principales preocupaciones es la pérdida de privacidad, ya que este malware puede recolectar información personal y datos de navegación, comprometiendo la privacidad del usuario. Además, existe el riesgo de exposición a malware, ya que Searchbox puede inyectar anuncios maliciosos en las páginas web visitadas, lo que puede llevar a la descarga de otros tipos de malware. Por último, el rendimiento del sistema también puede verse afectado, ya que el secuestrador consume recursos significativos del sistema, ralentizando su funcionamiento y causando errores y bloqueos en el navegador y el sistema en general.

## Impacto Financiero

El secuestrador de navegador Searchbox no solo tiene un impacto en la seguridad del sistema, sino también en el aspecto financiero de los usuarios y empresas afectados. En primer lugar, existen costos directos relacionados con el soporte técnico y la remediación de sistemas comprometidos, lo que puede resultar en gastos significativos. Además, la pérdida de productividad debido a la ralentización del sistema y la necesidad de limpiar el secuestrador también puede tener un impacto financiero negativo. Por otro lado, también existen costos indirectos, como el daño a la reputación de las empresas afectadas y la pérdida de confianza de los clientes debido a la recolección y posible exposición de datos personales.

## Consecuencias a Largo Plazo

Las consecuencias del secuestrador de navegador Searchbox pueden extenderse más allá del impacto inmediato en la seguridad y el aspecto financiero. Una de las principales preocupaciones a largo plazo es la vulnerabilidad a futuras infecciones, ya que la dificultad para eliminar completamente el malware puede dejar el sistema expuesto

a nuevos ataques. Además, si el secuestrador explota vulnerabilidades del sistema para persistir, puede dejar puertas abiertas para que otros atacantes aprovechen. Otra consecuencia a largo plazo es el deterioro del sistema, ya que las modificaciones realizadas por Searchbox pueden comprometer la integridad del sistema y requerir una reinstalación completa del sistema operativo para resolver completamente el problema. Esto puede resultar en una dependencia de herramientas de seguridad adicionales para protegerse contra futuras infecciones similares.

## Funcionamiento de SEARCHBOX

SEARCHBOX es una extensión maliciosa que se instala en el navegador del usuario mediante técnicas engañosas como el bundling o anuncios emergentes. Una vez instalado, modifica la configuración del navegador cambiando la página de inicio, la URL de nueva pestaña y el motor de búsqueda predeterminado a sitios fraudulentos. Además, realiza redirecciones forzadas a páginas promocionadas y utiliza técnicas para asegurarse de que el usuario no pueda revertir fácilmente los cambios realizados. Esto incluye la restricción del acceso a la configuración del navegador y la reinstalación automática de la extensión.

## Rastreo de Datos por SEARCHBOX

Una de las principales preocupaciones con SEARCHBOX es su capacidad para rastrear datos sensibles del usuario. Esta extensión recopila información como URLs visitadas, páginas web vistas, consultas de búsqueda, cookies, nombres de usuario/contraseñas e información financiera. Esta recopilación de datos puede tener graves consecuencias para la privacidad y seguridad de los usuarios, ya que puede ser vendida a terceros o utilizada para actividades maliciosas como el robo de identidad. Por lo tanto, es esencial tomar medidas inmediatas para eliminar SEARCHBOX y protegerse contra las amenazas que representa.

## Prevención de la instalación de SEARCHBOX

Para prevenir la instalación de SEARCHBOX en una red corporativa o doméstica, se pueden implementar diversas medidas. En primer lugar, es importante configurar políticas de seguridad en los navegadores para restringir la instalación de extensiones no verificadas. Además, se recomienda utilizar soluciones de seguridad como antivirus y antimalware que ofrezcan protección en tiempo real contra la instalación de software potencialmente no deseado. También es útil implementar filtros de contenido en la red para bloquear el acceso a sitios web maliciosos y servidores de anuncios engañosos que distribuyen este tipo de extensiones. Por último, es esencial educar a los usuarios sobre los riesgos asociados con la descarga de software desde fuentes no oficiales y el clic en anuncios emergentes o enlaces desconocidos. Con estas medidas, se puede prevenir la instalación de SEARCHBOX y proteger la red y los dispositivos contra esta amenaza.

Fernando Vargas Hincapié
https://www.alertasyseguridad.net/informes-reportes/