La mayoría de la compañías utilizan cookies para almacenar datos de los usuarios y utilizarlas en campañas de marketing digital, mediante la identificación de los intereses del usuario con las llamadas cookies de terceros. Esto permite también que compañías como Google o Facebook muestren anuncios más relevantes a los usuarios.

Pero esto podría representar algunos problemas, como en el caso del uso del antivirus Kaspersky, en el que se descubrió una vulnerabilidad que expuso un identificador único asociado al usuario con cada sitio web que visitó en los últimos cuatro años, lo que habría permitido que dichos sitios web y otros servicios de terceros rastreen al usuario en toda Internet, aún después de bloquear o borrar las cookies de terceros.

La vulnerabilidad, identificada como CVE-2019-8286 y descubierta por el investigador de seguridad independiente, Ronald Eikenberg, reside en la forma en que funciona un módulo de escaneo de URL integrado en el software antivirus, llamado Kaspersky URL Advisor.

De forma predeterminada, la solución de seguridad de Internet de Kaspersky inyecta un archivo JavaScript alojado remotamente en el código HTML de cada página web que se visita, para todos los navegadores web, incluso en el modo incógnito, en un intento por verificar si la página pertenece a la lista de sospechosos y direcciones web de phishing.

La mayoría de las soluciones de seguridad de Internet funcionan de forma similar para monitorear las páginas web en busca de contenido malicioso. Sin embargo, Eikenberg descubrió que la URL del archivo JavaScript contiene una cadena que es única para cada usuario de Kaspersky, una especie de UUID (Identificador Universalmente Único), que puede ser fácilmente capturado por sitios web, otros servicios de análisis y publicidad de terceros, poniendo la privacidad de los usuarios en riesgo.

> *«Es una mala idea porque otros scripts que se ejecutan en el contexto del dominio del sitio web pueden acceder al código HTML en cualquier momento y, por lo tanto, a la ID de Kaspersky inyectada. Lo que significa que cualquier sitio web simplemente puede leer la ID de Kaspersky del usuario y utilizarla para rastreo. Las*

> *ID fueron persistentes y no cambiaron después de varios días. Esto dejó en claro que una ID puede asignarse permanentemente a una computadora específica»*, dijo el investigador.

Eikenberg informó sus hallazgos a Kaspersky, misma que reconoció el problema y lo parchó el mes pasado asignando un valor constante (FD126C42-EBFA-4E12-B309-BB3FDD723AC1) para todos los usuarios en lugar de utilizar UUID en la URL de JavaScript.

> *«Kaspersky solucionó un problema de seguridad (CVE-2019-8286) en sus productos que podría comprometer la privacidad del usuario al utilizar una identificación única del producto que era accesible a terceros»,* dijo la compañía.
>
> *«Este problema se clasificó como divulgación de datos de usuario. El atacante debe preparar e implementar un script malicioso en los servidores web desde donde rastreará al usuario».*

Sin embargo, la función Kaspersky URL Advisor aún permite que los sitios web y servicios de terceros descubran si un visitante tiene instalado el software de Kaspersky en su sistema, lo que el investigador cree que los estafadores y cibercriminales pueden abusar directamente de él.

> *«Un atacante podría usar esta información para redistribuir una plaga adaptada al software de protección o redirigirla a una página de estafa adecuada, con el eslogan: su licencia de Kaspersky ha caducado. Ingrese su número de tarjeta de crédito para renovar la suscripción»*, dijo Eikenberg.

Las versiones actualizadas de los productos de Kaspersky Antivirus, Internet Security, Total Security, Free Antivirus y Small Office Security ya se han integrado a los usuarios afectados.

Sin embargo, los usuarios que deseen deshabilitar el seguimiento por completo, pueden hacerlo manualmente en la función del Asesor de URL desde la configuración > adicional > red > desmarcar el cuadro de procesamiento de tráfico.