Un script de huella digital en el navegador web es un fragmento de código JavaScript, que se ejecuta dentro de una página web y funciona probando la presencia de ciertas funciones del navegador.

Actualmente, los anunciantes en línea utilizan las huellas digitales del navegador como un mecanismo de seguimiento de usuarios de última generación.

Los anunciantes ejecutan distintos tipos de operaciones de recopilación de huellas digitales, crean una o más huellas para cada usuario y luego las utilizan para rastrear al usuario a medida que accede a otros sitios en Internet.

Debido a la forma intrusiva en la privacidad en la que los anunciantes utilizan actualmente las huellas digitales del navegador, varios desarrolladores como Firefox, Chrome, Opera, Brave y Tor, han implementado funciones para detectar y bloquear este tipo de código malicioso.

En un artículo publicado a inicios de agosto, un equipo de académicos de la Universidad de Iowa, Mozilla y la Universidad de California, Davis, analizó cómo los operadores de sitios web utilizan en la actualidad las secuencias de comandos de huellas digitales de los navegadores web más populares.

Mediante un kit de herramientas de aprendizaje automático que desarrollaron ellos mismos, llamado FP-Inspector, el equipo de investigación escaneó y analizó los 100 mil sitios web más populares en Internet, según el ranking de tráfico de Alexa.

> *«Descubrimos que las huellas dactilares del navegador ahora están presenten en más del 10% de los 100 mil sitios web principales y en más de una cuarta parte de los 10 mil sitios web principales»*, dijeron los investigadores.

Sin embargo, los investigadores también dijeron que a pesar de la gran cantidad de sitios que utilizan las huellas digitales del navegador, no todos los scripts se utilizan para el

seguimiento.

Algunas secuencias de comandos de huellas digitales también se utilizan para la detección de fraudes, ya que los bots automatizados tienden a tener huellas digitales iguales o similares, y las secuencias de comandos de huellas digitales son un método confiable para detectar el comportamiento automatizado.

Los investigadores también analizaron qué navegador o API de JavaScript presentaban las secuencias de comandos.

> *«Nuestra idea clave es que los scripts de huellas digitales del navegador normalmente no utilizan una técnica (por ejemplo, huellas digitales en lienzo) de forma aislada, sino que combinan varias técnicas juntas»*, dijeron los investigadores.

Ademas, identificaron grupos con técnicas de huellas digitales recurrentes, pero también grupos que contenían nuevas técnicas, que antes no se informaban como posibles vías de huellas digitales, lo que sugiere que las empresas están invirtiendo activamente en descubrir nuevas formas de rastrear a los usuarios según la huella de su navegador.

Entre las nuevas técnicas de toma de huellas digitales que se descubrieron, se resumen las siguientes:

- Huellas digitales de permisos: Los investigadores dijeron que algunos sitios web probaron la API de permisos del navegador, para determinar si el usuario otorgó o denegó un permiso. También dijeron que encontraron casos específicos en los que los scripts de huellas digitales habían sondeado si el usuario otorgó una notificación de sitio web, Geolocalización y acceso a la cámara, y estaban usando esta información para rastrear al usuario.
- Huellas digitales periféricas: Los investigadores dijeron que también encontraron scripts que investigaban si los sitios web habían recibido acceso para conectarse a

gamepads y dispositivos de realidad virtual, y estaban usando la información para rastrear a los usuarios. En otros casos, algunos sitios web tomaban las huellas digitales de los usuarios a través de la distribución de su teclado, normalmente expuesto a través de la función *getLayoutMap* del navegador.

- Huellas digitales de API: Los investigadores dijeron que algunos sitios web sondearon si el navegador del usuario tenía habilitadas API específicas. Por ejemplo, algunos scripts de huellas digitales verificaron la API de AudioWorklet (específica para navegadores Chromium), mientras que otros verificaron si ciertas funciones de JavaScript como *setTimeout o mozRTCSessionDescription* fueron anuladas por extensiones.
- Tiempo de toma de huellas digitales: Los investigadores también encontraron que algunos scripts de toma de huellas digitales medían el tiempo que tardaban en ejecutarse determinadas funciones. Por ejemplo, algunos sitios web utilizaron la API de rendimiento para realizar un seguimiento de los eventos como *domainLookupStart, domainLookupEnd, domInteractive y msFirstPaint* durante una operación predefinida.
- Huellas digitales de animación: Esta categoría es uno de los métodos de toma de huellas digitales más comunes actualmente, pero los investigadores dijeron que encontraron nuevas formas en que los sitios web están abusando de la API de AudioContext.
- Toma de huellas digitales de sensores: Al igual que las funciones relacionadas con la animación web, los sensores se han abusado mucho de los scripts de toma de huellas, pero el equipo de investigación dijo que encontraron sitios web que sondearon el sensor de proximidad del usuario, poco conocido.

Se pueden encontrar más detalles sobre la investigación en el artículo *«Fingerprinting the Fingerprinters: Learning to Detect Browser Fingerprinting Behaviors»,* que se presentará en el simposio IEEE sobre seguridad y privacidad, en mayo de 2021.

Los investigadores informaron la lista de dominios que alojaban scripts de huellas digitales descubiertos mediante FP-Inspector a Easylsit/EasyPrivacy y Disconnect, dos proyectos que administran las *«listas de bloqueo»*, que son una lista de dominios que se pueden cargar dentro de los bloqueadores de anuncios.