CNAME Cloaking es un práctica que consiste en difuminar la distinción entre cookies propias y de terceros, que no solo da como resultado la filtración de información privada confidencial sin el conocimiento y consentimiento de los usuarios, sino que también *«aumenta la superficie de amenazas de seguridad web»,* dijo un grupo de investigadores formado por Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen y Tom Van Goethem.

> *«Este esquema de seguimiento aprovecha un registro CNAME en un subdominio de modo que sea el mismo sitio que el sitio web incluido. Como tal, las defensas que bloquean las cookies de terceros se vuelven ineficaces»*, dijeron los investigadores.

Se espera que los hallazgos sean presentados en julio en el 21° Simposio de Tecnologías de Mejora de la Privacidad (PETS 2021).

Durante los últimos 4 años, todos los principales navegadores, con la excepción de Google Chrome, han incluido contramedidas para frenar el seguimiento de terceros.

Apple lanzó la función en Safari llamada Intelligent Tracking Protection (ITP) en junio de 2017, estableciendo un nuevo estándar de privacidad en computadoras de escritorio y dispositivos móviles para reducir el seguimiento entre sitios al *«limitar aún más las cookies y otros datos de sitios web».*

Dos años después, Apple esbozó un plan separado denominado *«Atribución de Clics en Anuncios que Preserva la Privacidad»* para hacer que los anuncios en línea sean privados.

Después, Mozilla comenzó a bloquear las cookies de terceros en Firefox de forma predeterminada a partir de septiembre de 2019, a través de una función denominada Protección de Seguimiento Mejorada (ETP), y en enero de 2020, el navegador Edge basado en Chromium de Microsoft hizo lo mismo. Luego, a fines de marzo de 2020, Apple actualizó ITP con bloqueo completo de cookies de terceros, entre otras características destinadas a evitar la toma de huellas dactilares de inicio de sesión.

Aunque Google anunció a inicios del año pasado sus planes para eliminar las cookies y los rastreadores de terceros en Chrome a favor de un nuevo marco llamado *«sandbox de privacidad»*, no se espera que entre en funcionamiento hasta 2022.

Mientras tanto, Google ha estado trabajando activamente con compañías de tecnología publicitaria en un reemplazo propuesto llamado «Dovekey«, que busca suplantar la funcionalidad ofrecida por el seguimiento entre sitios utilizando tecnologías centradas en la privacidad para publicar anuncios personalizados en la web.

Frente a estas barreras que eliminan las cookies para mejorar la privacidad, algunos especialistas en marketing comenzaron a buscar formas alternativas de evadir la postura absolutista adoptada por los fabricantes de navegadores contra el seguimiento entre sitios.

Los registros CNAME en DNS permiten mapear un dominio o subdiminio a otro, es decir, un alias, lo que los convierte en un medio ideal para contrabandear el código de seguimiento bajo la apariencia de un subdominio propio.

> *«Esto significa que el propietario de un sitio puede configurar uno de sus subdominios, como sub.blog.example, para resolverlo en thirdParty.example, antes de resolverlo con una dirección IP. Esto ocurre debajo de la capa web y se llama encubrimiento CNAME: el dominio thirdParty.example está encubierto como sub.blog.example y, por lo tanto, tiene los mismos poderes que el verdadero primer partido»*, explica el ingeniero de seguridad de Webkit, John Wilander.

En otras palabras, el encubrimiento de CNAME hace que el código de seguimiento parezca propio cuando en realidad no lo es, y el recurso se resuelve a través de un CNAME que difiere del dominio de origen.

No es sorprendente que este esquema de seguimiento esté ganando terreno rápidamente, creciendo un 21% en los últimos 22 meses.

Las cookies filtran información confidencial a los rastreadores

Los investigadores, en su estudio, encontraron que esta técnica se utiliza en el 9.98% de los 10,000 sitios web principales, además de descubrir 13 proveedores de dichos «servicios» de seguimiento en 10,474 sitios web.

Además, el estudio cita un *«tratamiento específico del navegador web de Apple, Safari»,* en el que la compañía de tecnología publicitaria Criteo cambió específicamente al encubrimiento de CNAME para evitar las protecciones de privacidad en el navegador.

Debido a que Apple ya implementó algunas defensas basadas en la vida útil para el encubrimiento de CNAME, es probable que el hallazgo refleje más los dispositivos que no ejecutan iOS 14 y macOS Big Sur, que admiten la función.

Lo más preocupante de las revelaciones es que se encontraron fugas de datos de cookies en 7377 sitios (95%) de los 7797 sitios que usaron el seguimiento CNAME, todos los cuales enviaron cookies que contienen información privada como nombres completos, ubicaciones, direcciones de correo electrónico e incluso, las cookies de autenticación a los rastreadores de otros dominios sin la afirmación explícita del usuario.

> *«En realidad, es incluso ridículo, porque ¿por qué el usuario daría su consentimiento para que un rastreador de terceros reciba datos totalmente no relacionados, incluidos los de naturaleza confidencial y privada?»*, dijo Olejnik.

Con muchos rastreadores CNAME incluidos a través de HTTP en lugar de HTTPS, los investigadores también plantean la posibilidad de que una solicitud que envíe datos analíticos al rastreador pueda ser interceptada por un adversario malintencionado en lo que

es un ataque de intermediario (MitM).

Además, la mayor superficie de ataque que supone la inclusión de un rastreador en el mismo sitio podría exponer los datos de los visitantes de un sitio web a la fijación de sesiones y ataques de secuencias de comandos entre sitios.

Los investigadores dijeron que trabajaron con los desarrolladores de rastreadores para abordar los problemas mencionados.

Mitigación del encubrimiento CNAME

Aunque Firefox no prohíbe el encubrimiento de CNAME inmediatamente, los usuarios pueden descargar un complemento como uBlock Origin para bloquear esos rastreadores de primera persona.

Cabe señalar que la compañía acaba de implementar Firefox 86 con Protección Total de Cookies, que evita el rastreo entre sitios al *«confirmar todas las cookies de cada sitio web en un tarro de cookies separado».*

Por otro lado, iOS 14 y Big Sur cuentan con protecciones adicionales que se basan en su función ITP para proteger el encubrimiento de CNAME de terceros, aunque no ofrece un medio para desenmascarar el dominio del rastreador y bloquearlo desde el principio.

> *«ITP ahora detecta solicitudes de encubrimiento de CNAME de terceros y limita el vencimiento de cualquier cookie establecida en la respuesta HTTP a siete días»,* dijo Wilander en un informe de noviembre de 2020.

Brave también hace lo mismo, y la semana pasada tuvo que publicar soluciones de emergencia para un error que surgió como resultado de agregar una función de bloqueo de anuncios basada en CNAME y en el proceso envió consultas para dominios .onion a los

resolutores públicos de DNS de Internet en lugar de utilizar nodos Tor.

Chrome y otros navegadores basados en Chromium se consideran como la única omisión, ya que no bloquean el encubrimiento de CNAME de forma nativa ni facilita que las extensiones de terceros resuelvan consultas de DNS obteniendo los registros CNAME antes de que se envíe una solicitud a diferencia de Firefox.

> *«La emergente técnica de rastreo CNAME evade las medidas anti-rastreo. Introduce serios problemas de seguridad y privacidad. Los datos del usuario se filtran, de forma persistente y constante, sin el conocimiento o consentimiento del usuario. Esto probablemente desencadena cláusulas relacionadas con GDPR y ePrivacy»*, dijo Olejnik.