El grupo de hackers de eGobbler que apareció en línea a inicios de este año con campañas masivas de publicidad maliciosa, ahora fue sorprendido ejecutando una nueva compaña que explota dos vulnerabilidades del navegador para mostrar anuncios emergentes intrusivos y redirigir a los usuarios a sitios web maliciosos.

Aún así, los piratas no han encontrado ninguna forma de publicar anuncios gratis, en cambio, el modus operandi de los atacantes de eGlobber implica altos presupuestos para mostrar miles de millones de impresiones de anuncios en sitios web de alto perfil por medio de redes publicitarias legítimas.

Pero en lugar de confiar en la interacción deliberada de los visitantes con los anuncios en línea, eGlobber utiliza exploits de navegador (Chrome y Safari) para lograr la tasa de clics máxima y secuestrar con éxito la mayor cantidad posible de sesiones de usuarios.

En su anterior campaña de publicidad maliciosa, el grupo eGlobber estaba explotando una vulnerabilidad de día cero (CVE-2019-5840) en Chrome para iOS en abril, lo que les permitió evitar con éxito el bloqueador de elementos emergentes incorporado en el navegador en dispositivos iOS y secuestrar 500 millones de sesiones de usuarios móviles en solo una semana para mostrar anuncios emergentes.

Aunque Google ya parchó la vulnerabilidad con el lanzamiento de Chrome 75 en junio, eGlobber sigue utilizando la falla para apuntar a quienes no han actualizado el navegador Chrome.

eGlobber aprovecha la falla de Webkit para redirigir a los usuarios a sitios web maliciosos

Sin embargo, el último informe publicado por la compañía de seguridad Confiant, los actores de estas amenazas descubrieron recientemente y comenzaron a explotar una nueva vulnerabilidad en Webkit, el motor del navegador utilizado por Apple Safari para iOS y MacOS, Chrome para iOS y también versiones anteriores de Chrome para escritorio.

El nuevo exploit de Webkit es más interesante porque no requiere que los usuarios hagan clic en ningún sitio de noticias legítimas, blogs o sitios web informativos que visitan, ni genera ningún anuncio emergente.

En cambio, los anuncios de display patrocinados por eGlobber aprovechan el exploit de Webkit para redirigir a los visitantes a sitios web que alojan esquemas fraudulentos o malware tan pronto como presionan el botón *«tecla abajo» o «página abajo»* en sus teclados mientras leen el contenido de la página web.

Esto se debe a que la vulnerabilidad de Webkit en realidad reside en una función de JavaScript, llamada evento onekyedown, que ocurre cada vez que un usuario presiona una tecla en el teclado, que permite que los anuncios que se muestran dentro de los iframes rompan las protecciones de sandbox de seguridad.

> *«Esta vez, sin embargo, la ventana emergente de Chrome de iOS no estaba apareciendo como antes, pero de hecho, estábamos experimentando redirecciones en los navegadores Webkit tras el evento onekeydown»*, dijeron los investigadores en su último informe.
>
> *«La naturaleza del error es que un iframe anidado de origen cruzado puede enfocarse automáticamente, lo que evita la directiva de espacio aislado 'allow-top-navigation-by-user-activation' en el marco primario. Con el marco interno enfocado automáticamente, el evento keydown se convierte en un evento de navegación activado por el usuario, lo que hace que el sandboxing de anuncios sea completamente inútil como medida para la mitigación de redireccionamiento forzado»,* agregaron.

Aunque la pautas de la tienda de aplicaciones de Apple restringen todas las apps de iOS con capacidad de navegación web para usar su marco Webkit, incluido Google Chrome para iOS, los usuarios de dispositivos móviles aún tienen menos probabilidades de verse afectados por

la falla de redirección, ya que el evento onekydown no funciona en el sistema operativo móvil.

Sin embargo, la carga útil de eGlobber, a menudo entregada por medio de servicios CDN populares, también incluye código para activar redirecciones cuando los visitantes de una aplicación web específica intentan ingresar algo en un área de texto o formularios de búsqueda, probablemente *«para maximizar las posibilidades de secuestrar estas pulsaciones de teclas»*.

Entre el 1 de agosto y el 23 de septiembre, se ha visto a los actores de amenazas sirviendo su código malicioso a un gran volumen de anuncios, que los investigadores estiman en hasta 1.16 mil millones de impresiones.

Mientras que la anterior campaña de publicidad maliciosa de eGlobber se dirigió principalmente a usuarios de iOS en Estados Unidos, el último ataque se dirigió a usuarios en países de Europa, siendo la mayoría de Italia.

Confiant informó en privado la vulnerabilidad de Webkit a los equipos de seguridad de Google y Apple. Apple solucionó la falla en Webkit con el lanzamiento en iOS 13 el 19 de septiembre y en el navegador Safari 13.0.1 el 24 de septiembre, mientras que Google no ha solucionado el problema en Chrome.