Como una forma de proteger a sus usuarios con sede en Kazajstán de la vigilancia del gobierno, Google, Apple y Mozilla finalmente se presentaron y bloquearon el certificado raíz de CA emitido por el gobierno de Kazajstán dentro de su respectivo software de navegación web.

A partir de ayer, los usuarios de Chrome, Safari y Firefox en Kazajstán verán un mensaje de error que indica que no se debe confiar en el certificado *«Quaznet Trust Network»* al intentar acceder a un sitio web correspondiente con el certificado emitido por el gobierno.

Hace un mes se informó que todos los principales proveedores de servicios de Internet de Kazajstán están obligando a sus clientes a instalar un certificado raíz emitido por el gobierno en sus dispositivos para recuperar el acceso a sus servicios de Internet.

El certificado raíz, etiquetado como *«Certificado de Confianza» o «Certificado de Seguridad Nacional»,* si está instalado, permite a los ISP interceptar, monitorear y descifrar las conexiones HTPPS y TLS cifradas de los usuarios, ayudando al gobierno a espiar a sus 18 millones de personas y censurar contenido.

Una vez instalado, el certificado permitió al gobierno kazajo descifrar y leer cualquier cosa que un usuario haya visitado, incluyendo redes sociales, además de interceptar la información y contraseñas de las cuentas.

> *«Cuando un usuario en Kazajstán instala el certificado raíz proporcionado por su ISP, elige confiar en una CA que no tiene que seguir ninguna regla y puede emitir un certificado para cualquier sitio web a cualquier persona. Esto permite la intercepción y descifrado de las comunicaciones de red entre Firefox y el sitio web, a veces denominado ataque de Monster in the Middle (MITM)»*, dice Mozilla.

La instalación del certificado raíz de CA personalizado no solo le permite al gobierno vigilar

las actividades en línea de sus ciudadanos, sino que también los expone al riesgo de ataques de ingeniería social como una oportunidad para que los hackers engañen a los usuarios para instalar un certificado raíz malicioso de sitios web y fuentes no confiables.

Después de enfrentar críticas mundiales, el gobierno kazajo describió la implementación inicial del certificado como una prueba para monitorear las amenazas cibernéticas y luego abandonó sus planes para interceptar el tráfico de Internet de los ciudadanos.

> *«Nunca toleraremos ningún intento, por parte de ninguna organización, gubernamental o de otro tipo, de comprometer los datos de los usuarios de Chrome. Hemos implementado protecciones contra este problema específico y siempre tomaremos medidas para proteger a nuestros usuarios en todo el mundo. Los usuarios no necesitan ninguna acción para estar protegidos. Además, el certificado se agregará a una lista de bloqueo en el código fuente de Chromium, por lo que deberían incluirse en otros navegadores basados en Chromium a su debido tiempo»,* dijo Parisa Tabriz, Directora Senior de Ingeniería de Chrome.

Aunque Apple no ha realizado ninguna publicación al respecto, un portavoz de la compañía contactó a THN para confirmar que su navegador web Safari también bloquea el certificado raíz de CA emitio por el gobierno de Kazajstán.

> *«Apple cree que la privacidad es un derecho humano fundamental, y diseñamos cada producto Apple desde cero para proteger la información personal. Hemos tomado medidas para garantizar que Safari no confíe en el certificado y nuestros usuarios estén protegidos de este problema»,* dijo un portavoz de Apple por correo electrónico.

Esta no es la primera vez que el gobierno de Kazajstán intercepta el tráfico de Internet de sus ciudadanos. En 2015, el gobierno emitió incluir un certificado raíz de confianza de Mozilla,

pero la compañía rechazó la solicitud tan pronto como se descubrió que el gobierno de Kazajstán tenía la intención de usar dicho certificado para interceptar los datos de los usuarios.

Google y Mozilla recomiendan eliminar el certificado raíz del gobierno de Kazajstán de sus dispositivos y cambiar las contraseñas para cada una de sus cuentas.