El gobierno de Kazakhstan emitió una vez más un aviso a todos los principales proveedores locales de servicios de Internet (ISP) pidiéndoles que hagan obligatoria la instalación de certificados raíz emitidos por el gobierno a todos sus usuarios, para poder recuperar el acceso a los servicios de Internet.

El certificado raíz en cuestión, etiquetado como *«certificado de confianza»* o *«certificado de seguridad nacional»,* al estar instalado, permite a los IPS interceptar y monitorear las conexiones HTTPS y TLS cifradas de los usuarios, lo que ayuda al gobierno a espiar a sus ciudadanos y censurar el contenido.

En resumen, el gobierno prácticamente está lanzando un ataque *«man in the middle»* a sus propios ciudadanos.

Normalmente, cualquier dispositivo o navegador web confía automáticamente en los certificados digitales emitidos solo por una lista específica de Autoridades de Certificación (CA) que tienen sus certificados raíz instalados en su sistema.

Por lo tanto, obligar a los usuarios de Internet a instalar un certificado raíz que pertenece a una Organización de Gobierno les da autoridad para generar certificados digitales válidos para cualquier dominio que quieran interceptar por medio de su tráfico HTTPS.

A partir de abril de este año, los proveedores de servicios de Internet kazajos, comenzaron a informar a sus usuarios sobre el *«certificado de seguridad nacional»,* que sería obligado a instalar para poder seguir con el acceso ininterrumpido a una listo de sitios web HTTPS permitidos.

Tele2, uno de los principales proveedores de servicios de Internet kazajos, finalmente comenzó a redirigir todas las conexiones HTTPS de sus clientes a una página web que contiene archivos de certificados e instrucciones sobre cómo instalarlos en dispositivos con Windows, MacOS, Android e iOS.

Una de las implicaciones de seguridad más graves que se puede detectar en esto, es que

debido a que los usuarios solo pueden navegar por sitios que no son HTTPS antes de instalar los certificados, los archivos Cert están disponibles para descargar solo a través de conexiones HTTP inseguras, lo que permite a los hackers reemplazar fácilmente el archivo de certificado utilizando ataques MiTM.

Otros ISP nacionales, que se lista a continuación, también tienen planes para obligar a sus usuarios de Internet a instalar el certificado raíz en breve para cumplir con las leyes.

- Beeline
- K-Cell
- Active
- Altel
- Kazakhtelecom

El controvertido aviso se emitió con respecto a las enmiendas a la Ley de Comunicaciones de 2004, que el gobierno de Kazajstán aprobó en noviembre de 2015.

Según la cláusula 11 del artículo 26, *«Reglas Para Emitir y Aplicar un Certificado de Seguridad»*, todos los proveedores de servicios de comunicaciones nacionales están obligados a monitorear el tráfico de Internet cifrado de sus clientes utilizando certificados de seguridad emitidos por el gobierno.

Se pretendía que la ley entrara en vigencia a partir del 1 de enero de 2016, pero el gobierno de Kazajstán no forzó a los ISP locales después de una serie de demandas.

Ahora, el gobierno de Kazajstán está haciendo otro intento por forzar las enmiendas, poniendo en riesgo la privacidad y la seguridad de millones de sus ciudadanos, tanto por parte de piratas informáticos como del propio gobierno al romper los fundamentos del protocolo de seguridad de Internet.

Según la nota mostrada por los proveedores de Internet, las enmiendas fueron forzadas *«en relación a los frecuentes casos de robo de datos personales y credenciales, así como el*

dinero de las cuentas bancarias de Kazajstán».

> *«Se ha introducido un certificado de seguridad que se convertirá en una herramienta eficaz para proteger el espacio de información del país de los piratas informáticos, los estafadores de Internet y otros tipos de amenazas cibernéticas»,* dice la nota.
>
> *«La introducción de un certificado de seguridad ayudará también a la protección de los sistemas de información y datos, así como en la identificación de hackers y estafadores de Internet antes de que puedan causar daños».*
>
> *«Además, permitirá a los usuarios de Internet de Kazajstán estar protegidos contra ataques de piratas informáticos y ver contenido ilegal».*

Con estas declaraciones, es evidente que el gobierno kazajo quiere tomar el control sobre el contenido que sus ciudadanos deberían ver en Internet y también convertir a KAzajstán en un estado de vigilancia profunda.

Además, el espionaje de comunicaciones HTTPS también permitirá a los ISP inyectar publicidades o rastrear scripts en todas las páginas web que los usuarios visiten.

Por ahora no está claro cómo las principales empresas de tecnología y los navegadores web responderán a esta nueva infracción de privacidad de los ciudadanos kazajos.