El gobierno ruso estableció su propia autoridad de certificación TLS (CA) para abordar los problemas de acceso a sitios web que surgieron a raíz de las sanciones impuestas por Occidente luego de la invasión militar no provocada de Ucrania por parte de Rusia.

Según un mensaje publicado en el portal de servicios públicos Gosuslugi, se espera que el Ministerio de Desarrollo Digital proporcione un reemplazo nacional para manejar la emisión y renovación de los certificados TLS en caso de que sean revocados o vencidos.

El servicio se ofrece a todas las entidades legales que operan en Rusia, y los certificados se entregan a los propietarios de los sitios previa solicitud dentro de 5 días hábiles.

Los certificados TLS se usan para vincular de forma digital una clave criptográfica a los detalles de una organización, lo que permite que los navegadores web confirmen la autenticidad del dominio y garanticen que la comunicación entre una computadora cliente y el sitio web de destino sea segura.

La respuesta se produce cuando a empresas como DigiCert se les restringe hacer negocios en Rusia tras las sanciones de las naciones occidentales.

> *«La validación de los pedidos rusos puede demorar más en procesarse debido a los extensos controles requeridos para empresas y personas privadas, sin embargo, podemos ofrecer todos los productos a este país»,* dijo la compañía en un aviso.

Lo que no está claro aún es si los navegadores web como Google Chrome, Microsoft Edge, Mozilla Firefox y Apple Safari, tienen la intención de aceptar los certificados emitidos por la nueva autoridad de certificación rusa para que las conexiones seguras a los servidores certificados puedan funcionar según lo previsto.

Pero según informó Juan Andrés Guerrero-Saade, investigador principal de amenazas de SentinelOne, la agencia de servicios públicos recomienda el uso de navegadores rusos como Yandex y Atom, para *«tener acceso a todos los sitios y los servicios en línea necesarios,*

*incluidos los servicios públicos, recomendamos instalar navegadores que admitan el certificado ruso»*, dijo en un correo electrónico.

Esto también presenta riesgos significativos en el sentido de que podría armarse potencialmente para llevar a cabo operaciones de intermediario (MitM) en sesiones HTTPS que se originan en usuarios de Internet en la nación, lo que permite a las autoridades pertinentes interceptar, descifrar y volver a cifrar el tráfico que pasa por sus sistemas.

Este desarrollo también se acerca a las revelaciones de Cisco Talos de que los ciberdelincuentes oportunistas se aprovechan del conflicto en curso para apuntar a usuarios involuntarios que buscan herramientas para llevar a cabo sus propios ataques cibernéticos contra entidades rusas al ofrecer malware que pretende ser herramientas cibernéticas ofensivas.

> *«El interés global en el conflicto crea un enorme grupo de víctimas potenciales para los actores de amenazas y también contribuye a que haya un número creciente de personas interesadas en llevar a cabo sus propias operaciones cibernéticas ofensivas»,* dijeron los investigadores.

> *«Estas observaciones sirven como recordatorios de que los usuarios deben estar en alerta máxima ante una mayor actividad de amenazas cibernéticas a medida que los actores de amenazas buscan nuevas formas de incorporar el conflicto entre Rusia y Ucrania en sus operaciones»,* agregaron.