El gobierno de Estados Unidos volvió a advertir este lunes sobre posibles ataques cibernéticos de Rusia en represalia por las sanciones económicas impuestas por Occidente al país, luego de su asalto militar a Ucrania el mes pasado.

> *«Es parte del libro de jugadas de Rusia. Inteligencia en evolución de que el gobierno ruso está explotando opciones»*, dijo el presidente de Estados Unidos, Joe Biden.

El desarrollo se produce cuando la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), y la Oficina Federal de Investigaciones (FBI), advirtieron sobre *«posibles amenazas»* para las redes de comunicación satelital internacional y de Estados Unidos (SATCOM) a raíz de un ataque cibernético dirigido a la red Viasat KA-SAT, utilizada ampliamente por el ejército ucraniano, aproximadamente en la época en que las fuerzas armadas rusas invadieron Ucrania el 24 de febrero.

> *«Las intrusiones exitosas en las redes SATCOM podrían crear un riesgo en los entornos de clientes de los proveedores de redes SATCOM»*, dijeron las agencias.

Para fortalecer las defensas de seguridad cibernética contra la actividad cibernética maliciosa, el gobierno recomienda a las organizaciones que exijan el uso de la autenticación multifactor, se aseguren de que los sistemas estén actualizados y parcheados contra todas las vulnerabilidades conocidas, cifren los datos en reposo y mantengan copias de seguridad fuera de línea.

> *«Construya seguridad en sus productos desde cero, 'hornéelo, no lo atornille', para proteger tanto su propiedad intelectual como la privacidad de sus clientes»*, dijo el gobierno de Estados Unidos.

Esto al mismo tiempo que instó a las empresas a examinar la procedencia de componentes

de software, de código abierto o de otro tipo, para estar atento a las amenazas de la cadena de suministro.

CERT-UA emite alerta

Las advertencias sobre incidentes indirectos siguen a un conjunto de ataques cibernéticos que han afectado tanto a Ucrania como a Rusia en las últimas semanas (aunque han sido muy silenciados en comparación con lo contrario). Rusia, por su parte, instó a las empresas nacionales a desactivar las actualizaciones automáticas de software y cambiar a servidores DNS rusos.

La semana pasada, el Equipo de Respuesta a Emergencias Informáticas de Ucrania (CERT-UA), también notificó sobre nuevas campañas de phishing dirigidas a entidades estatales con el objetivo de implementar una puerta trasera llamada LoadEdge. La agencia atribuyó los ataques a InvisiMole, un equipo de hackers con presuntos vínculos con el grupo estatal nacional con sede en Rusia, Gamaredon.

Por separado, el CERT-UA alertó que los sistemas de información de las empresas ucranianas están siendo comprometidos por un programa de limpieza basado en C# llamado DoubleZero, que está diseñado para sobrescribir todos los archivos que no son del sistema y hacer que las máquinas dejen de funcionar.

Además, la tendencia emergente de usar «protestware» para envenenar bibliotecas de código abierto ampliamente utilizadas como una forma de condenar la guerra, ha generado temores de que podría dañar sistemas críticos y socavar la confianza en la seguridad de la cadena de suministro de software y el ecosistema de código abierto.

Como consecuencia, el banco estatal ruso Sberbank, aconsejó a los usuarios que abandonen temporalmente las actualizaciones de software, además de pedir a los *«desarrolladores que aumenten el control sobre el uso de código fuente externo y realicen una verificación manual o automática, incluida la visualización del texto del código fuente»*, dijo el servicio estatal de noticias TASS.

Fugas de la versión 3 de Conti

Además, la invasión rusa de Ucrania también se ha manifestado en forma de esfuerzos hacktivistas de colaboración colectiva para participar en una variedad de acciones digitales contra Rusia, principalmente apoyándose en ataques DDoS y publicando grandes cantidades de información corporativa confidencial.

El principal en la lista es un investigador de seguridad ucraniano anónimo apodado @ContiLeaks, que filtró el código fuente del ransomware Conti con sede en Rusia, incluida la más reciente *«versión 3»*, así como casi 170,000 conversaciones internas de chat entre los pandilleros a inicios del mes, después de que el grupo se pusiera del lado de Rusia.

Por otro lado, el tribunal de distrito de Tverskoy de Moscú, prohibió las plataformas de redes sociales propiedad de Meta, Facebook e Instagram, por participar en *«actividades extremistas»,* prohibiendo a la empresa hacer negocios en el país con efecto inmediato. El fallo sigue a una decisión temporal por parte de Meta que permite a los usuarios de Europa del Este publicar contenido que llame a la violencia contra los soldados rusos.