Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

IFX NETWORKS BAJO ATAQUE DE RANSOMWARE

13/Septiembre/2023

CONTENIDO

INTRODUCCIÓN

Varias páginas web de entidades del Gobierno nacional, superintendencias y de la rama judicial en Colombia, se encuentran caídas por suspensión del servicio de la compañía multinacional IFX Networks, que tuvo que activar su sistema de seguridad luego de identificar un ataque cibernético Ransomware en sus máquinas.

IFX NETWORKS BAJO ATAQUE DE RANSOMWARE

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2023_09_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alto
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/09/2023
Es día cero (0 day):	Si

RESUMEN

Varias páginas web de entidades del Gobierno nacional, superintendencias y de la rama judicial en Colombia, se encuentran caídas por suspensión del servicio de la compañía multinacional IFX Networks, que tuvo que activar su sistema de seguridad luego de identificar un ataque cibernético Ransomware en sus máquinas.

El ataque a las máquinas de soporte en Colombia también ha afectado la prestación de servicios en otros países de Latinoamérica. La compañía, que presta el servicio tecnológico a varias entidades del Gobierno colombiano y otros 17 países de la región, informó que sobre las 5:50 a.m. del 12 de septiembre la nube "recibió un ataque de ciberseguridad externo tipo Ransomware, afectando algunas de sus máquinas virtuales".

Sobre las 9 de la noche, cuando se confirmó la situación, IFX señaló que continuaba trabajando ante la incidencia, pero aclaró que no había reportado vulnerabilidad en la información, privacidad y seguridad de los datos alojados en la nube, debido a que cuentan con protocolos de seguridad que no se habrían visto afectados.

Sin embargo, el ataque sí generó que se cayeran varias páginas que tienen soporte digital en la nube de la multinacional. “La Supersalud informa que el proveedor IFX de la entidad está presentando una falla masiva que afecta el acceso a nuestros sistemas NRVCC, Supercor y sitio web”, informó la entidad, adscrita al Ministerio de Salud, a las 4:45 p.m. del 12 de septiembre.

Supersalud alerta por falla generalizada en sus servicios tecnológicos

Bogotá, 12 de septiembre de 2023. La Superintendencia Nacional de Salud informa a sus grupos de interés, vigilados y usuarios en general que desde las 6:00 de la mañana de hoy se presentan fallas en la disponibilidad de servicios tecnológicos, con lo cual no se puede acceder al portal web de la Superintendencia y a algunos de sus aplicativos de uso externo e interno.

Estos servicios tecnológicos están alojados en la infraestructura que la Supersalud tiene contratada con la firma IFX NETWORKS COLOMBIA S.A.S y se está a la espera de una evaluación que permita determinar la duración en la falla de disponibilidad.

La afectación cobija también el acceso a la plataforma donde se radican las quejas y la correspondencia, así como los sistemas de gestión de auditorías, de inventarios, de control de las entidades que se encuentran en medidas especiales y de recepción y validación de archivos, entre otros procesos y aplicativos.

Desde la Superintendencia, la Subdirección de Tecnologías de la Información está adelantando las acciones necesarias para la verificación, validación y puesta en funcionamiento de los sistemas y servicios indicados, y tiene conocimiento que dificultades similares suceden con entidades que cuentan con el mismo proveedor.

CP-OCEII-108

La Rama Judicial confirmó que desde la fecha en la que se registró el ataque, se presentaron problemas en el funcionamiento de varias de sus páginas que tienen respaldo en la multinacional. El Consejo Superior de la Judicatura notificó a los funcionarios del fallo e indicó las páginas que sí estaban en funcionamiento. Sin embargo, la radicación de tutelas y la firma virtual de los jueces se ha visto afectada.

“La Unidad de Informática de Dirección Ejecutiva de Admón Judicial trabaja en el restablecimiento del portal web y algunos sistemas de la Rama Judicial, los cuales han presentado fallas en los servicios que presta el sitio web. Estaremos informando cuando se normalice el servicio”, señaló la institución.

La afectación se extiende también a varias páginas institucionales del Ministerio de Cultura tanto la principal de la entidad como el Museo Nacional, la Biblioteca Nacional, varios proyectos y espacios culturales, como también en el portal del Museo Nacional de Memoria Histórica. A estos se suman varias empresas privadas y farmacéuticas que señalan haberse quedado sin sistema desde el 12 de septiembre.

Algunas de las páginas afectadas del Ministerio de Cultura son:

En Chile, donde IFX Networks también presta servicios, el Equipo de Respuesta ante Incidentes de Seguridad Informática del Ministerio del Interior señaló que varios portales quedaron indisponibles. Desde la entidad emitieron una alerta a raíz del comunicado de la multinacional.

Desde IFX Networks señalaron que identificaron “un evento de un Ransomware en algunas de nuestras máquinas virtuales de Colombia. Hasta el momento no se ha evidenciado un compromiso a la integridad de los datos ni de la información de sus clientes, proveedores y sobre todo en Chile, y demás grupos relacionados”. Uno de los afectados por la caída de los servicios, fue el portal chileno de compras públicas, es así, que urante la tarde Chilecompra emitió un comunicado informando que “debido a un problema del proveedor de infraestructura tecnológica IFX Networks que afecta a todos sus clientes en Latinoamérica, la plataforma de compras públicas www.mercadopublico.cl, no se encuentra actualmente disponible”.

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).
- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.
- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión.
- Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red

NOTICIA COMPLETA

https://devel.group/blog/ifx-networks-bajo-ataque-de-ransomware/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente