República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Informe

Número: IF-2023-44348101-APN-GAIRI#SSN

CIUDAD DE BUENOS AIRES
Jueves 20 de Abril de 2023

Referencia: Comunicación a las Cámaras y Asociaciones del Sector

---

A las Cámaras y Asociaciones del Sector:

Nos dirigimos a fin de proporcionar información técnica y de contexto sobre el evento que afectara a la SSN, el cual impactó en la disponibilidad de los servicios informáticos del Organismo.

A continuación se describen los elementos principales observados a la fecha, consignando que la SSN se encuentra trabajando activamente en el proceso de recuperación y restablecimiento de los servicios afectados.

CONTEXTO GENERAL

El 03 de abril la SSN detectó un evento de seguridad informática, catalogado como ciberataque con ejecución de un ransomware, el cual impactó a distintos recursos informáticos de la red interna del organismo y afectó sus sistemas e información allí alojada.

En forma inmediata, la SSN puso en marcha un proceso de análisis de impacto y de recuperación de sus servicios informáticos, para el cual dispuso recursos técnicos y humanos propios y de terceros, especializados en la recuperación de este tipo de eventos.

Como parte del proceso de respuesta, se conformó un Comité de Crisis que coordina la ejecución de las acciones necesarias a fin de restablecer el funcionamiento de los sistemas y servicios informáticos del Organismo.

Cabe destacar que la SSN procedió a realizar la denuncia correspondiente el día 10 de abril frente a la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Ministerio Público Fiscal. Actualmente tramita en el Juzgado Criminal y Correccional Federal 1 y su seguimiento está bajo la órbita de la Gerencia de Asuntos Jurídicos del Organismo.

INFORMACION RELEVANTE

La SSN sufrió un evento informático a partir de acciones ejecutadas por un grupo de ciber atacantes internacionales, que incluyó la ejecución de un ransomware de la familia “D0NUT“. Este ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado.

Conforme se avanzó en el análisis de los impactos técnicos y del ciberataque, hasta el momento no se pudo identificar que los ciber atacantes hubieran realizado otras acciones maliciosas significativas ni que hubieran extraído información de la SSN; ni que el ransomware específico que afectó a SSN se hubiera propagado y/o afectado a terceras partes conectadas.
Asimismo, a la fecha no fue publicada información sobre el evento que afectó a SSN por parte del actor malicioso/ransomware D0NUT.

CONTENCIÓN DEL EVENTO

Estamos trabajando en el proceso de recuperación de los principales servicios informáticos de la SSN y poniendo en marcha planes de continuidad operativa para aquellos servicios que por razones técnicas aún no puedan ser recuperados.

Las acciones inmediatas de contención del evento de ransomware ejecutadas por la SSN incluyeron lo siguiente:

- Desconexión de equipos encriptados para evitar su propagación
- Limitación de los accesos remotos a la red informática de SSN
- Inicio de las tareas de recuperación de servicios y aplicaciones en un segmento de red seguro
- Inicio de las tareas de continuidad operativa de procesos críticos

Por último, queremos confirmar que cualquier avance o actualización de la información así como también cualquier elemento técnico relevante será comunicado y compartido oportunamente.

Quedando a disposición para aclarar cualquier consulta sobre el presente, saluda atentamente

Digitally signed by Gestion Documental Electronica
Date: 2023.04.20 16:12:23 -03:00

Maria Veronica Lopez Quesada
Gerenta
Gerencia de Asuntos Institucionales y Relaciones Internacionales
Superintendencia de Seguros de la Nación

Digitally signed by Gestion Documental Electronica
Date: 2023.04.20 16:12:23 -03:00