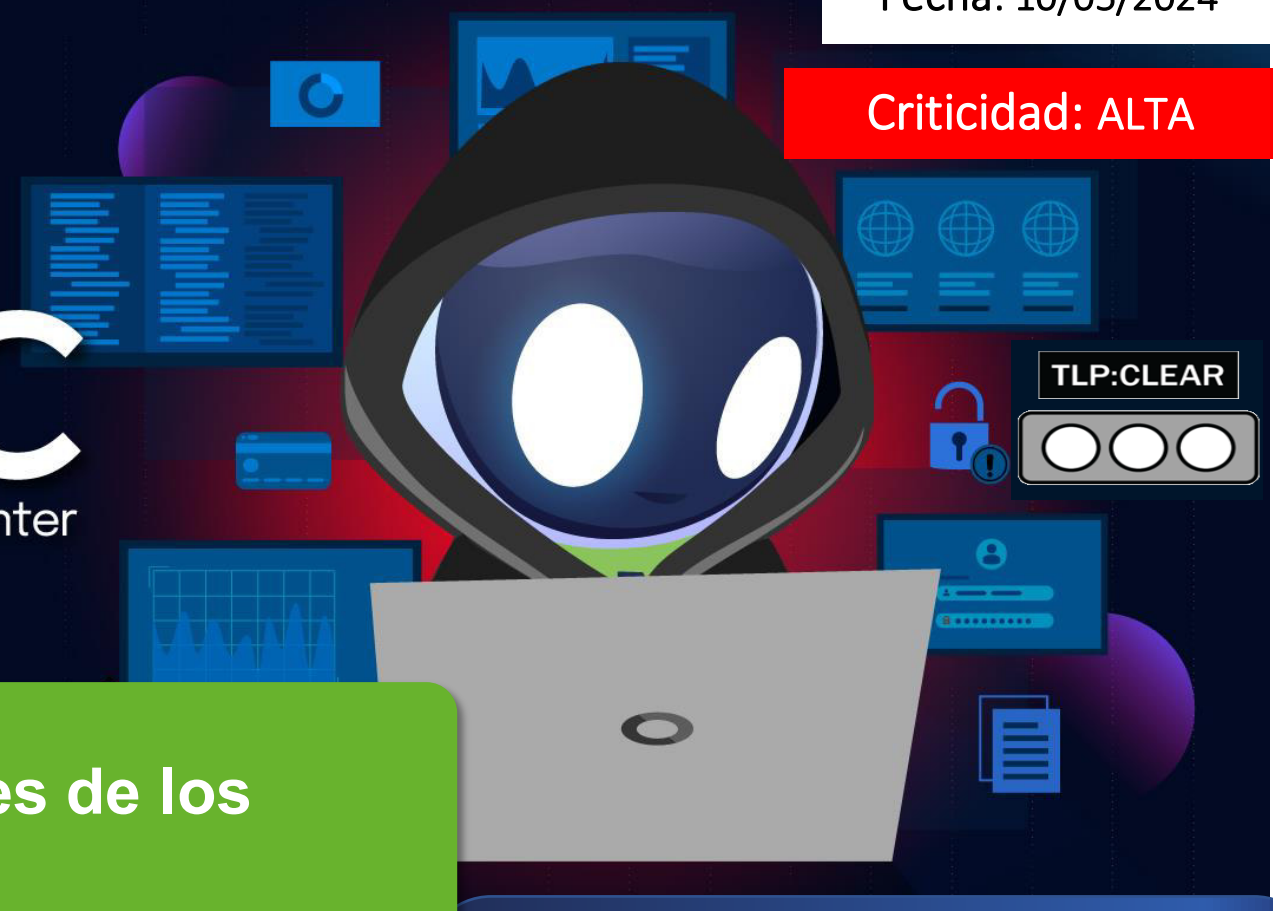
multisoft 30 Años
Soluciones en Movimiento

NGSOC
Next Generation Security Operation Center

Fecha: 10/05/2024

Criticidad: ALTA



Exposición de datos sensibles de los usuarios de seguros Sura.

DESCRIPCIÓN DE LA AMENAZA:

De acuerdo con el monitoreo realizado por el equipo SOC en los distintos medios digitales, se da a conocer una posible exposición de datos, en el cual, el pasado 8 de mayo, se publicaron en un foro de venta de bases de datos las supuestas pruebas del robo y exposición de datos de clientes de Sura Seguros. Un actor malicioso afirma haber subido a un repositorio una cantidad no identificada de datos robados.

La información comprometida podría incluir datos personales, financieros y de contacto de los clientes de Sura Seguros. La magnitud exacta del robo y la naturaleza de los datos expuestos aún no se ha determinado.

Sura Seguros ha emitido un comunicado oficial confirmando el incidente y señalando que están tomando las medidas necesarias para investigar la situación y proteger la información de sus clientes. La compañía ha informado que ha contratado a expertos en seguridad informática para investigar el incidente y que está trabajando con las autoridades competentes.

VIDA_GRUPO	699,342,616	609,031,867	File folder	8/25/2021 4:11 ...
MAYO	777,105	529,677	File folder	5/6/2024 1:21 ...
MARZO	25,292,713	21,502,219	File folder	3/5/2024 3:02 ...
FEBRERO	19,492,294	16,068,431	File folder	2/6/2024 2:40 ...
EMPRESARIALES	13,406,672	10,429,056	File folder	11/6/2020 8:23 ...
AUTOS	0	0	File folder	10/16/2020 4:5...
ABRIL	19,360,880	16,356,787	File folder	4/6/2024 2:12 ...
091	7,305,810	6,275,496	File folder	4/21/2021 6:52 ...

Imagen 1: Datos expuestos. Fuente: Muchohacker

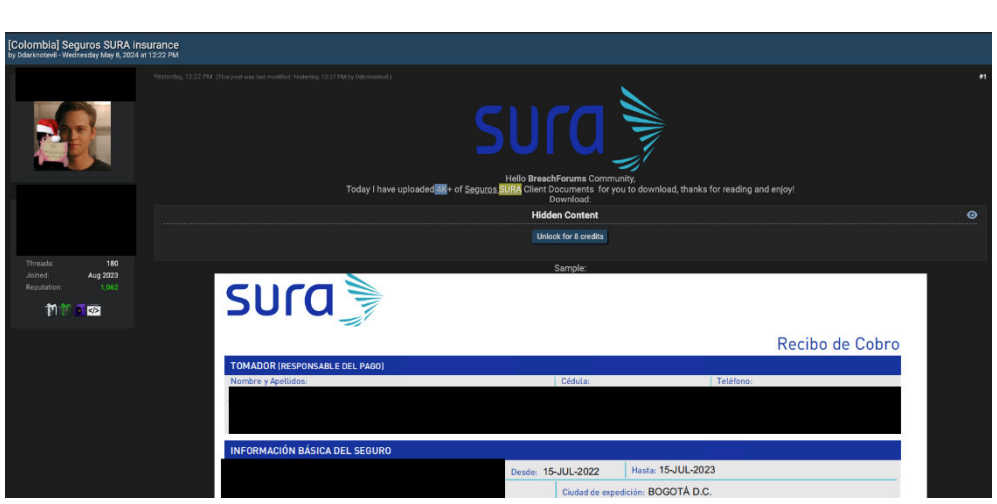


Imagen 2: Prueba de la información robada a la organización. Fuente: Mucho hacker

Sector afectado: **General**

Recomendaciones y Mitigación

- **Monitorear la actividad de la información de la compañía**
- **Implementar un sistema de DLP en la organización.**
- **Realizar monitoreo en la red de la organización.**
- **Se recomienda cambio de credenciales periódicamente.**

Referencias

- https://muchohacker.lol/2024/05/violacion-de-privacidad-datos-confidenciales-de-clientes-de-sura-seguros-expuestos/