multisoft 30 Años
Soluciones en Movimiento

NGSOC
Next Generation Security Operation Center

Fecha: 16/05/2024

Criticidad: ALTA

Alerta de ciberataque a empresa colombiana por parte del grupo ransomware DragonForce

DESCRIPCIÓN DE LA AMENAZA:

De acuerdo con el monitoreo realizado por el equipo SOC en los distintos medios digitales, se ha logrado identificar que el grupo de Ransomware DragonForce, ha tenido 4 víctimas nuevas, entre las cuales se encuentra la empresa colombiana Altipal S.A.S.

El grupo Ransomware DragonForce, ha publicado en un foro donde menciona que logro robar 183.7 Gb de data de Altipal S.A.S, empresa dedicada a prestar servicios de marketing.

La forma en la que operar este grupo, es por medio de técnicas de doble extorsión con el fin de exfiltrar y cifrar datos. Además, puede finalizar procesos para facilitar el cifrado más rápido. Una vez comprometido un sistema, el ransomware cambia el nombre de los archivos afectados y deja instrucciones de rescate en cada directorio.

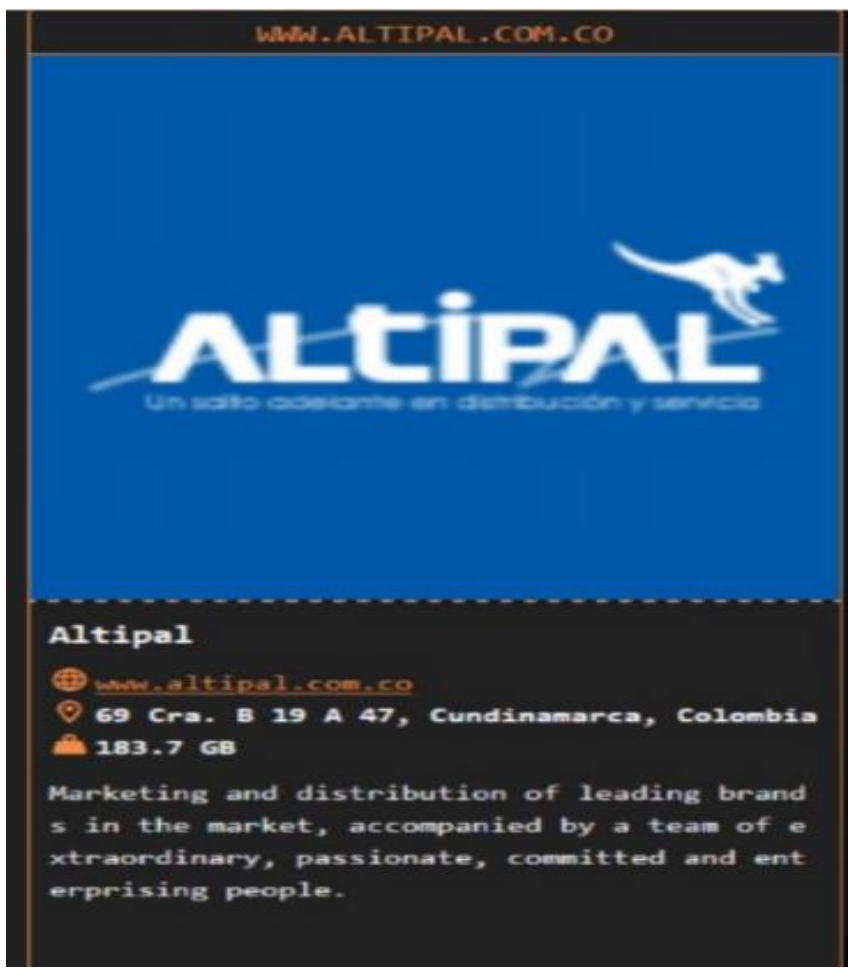

Imagen: Informacion expuesta. Fuente: https://twitter.com/falconfeedsio

Sector afectado: **General**

Recomendaciones y Mitigación

- **Se recomienda a las empresas que implementen medidas de seguridad sólidas para protegerse de ataques de Ransomware, como copias de seguridad regulares, capacitación en seguridad para empleados y soluciones de seguridad de Endpoint.**

- **Tener sistema de DLP que controle la información sensible de la compañía.**
- **Tener una estrategia de ciberseguridad, que permita minimizar el riesgo de fuga de la información de la compañía.**

Referencias

- https://twitter.com/falconfeedsio/status/1790366456812908944?s=46