SIO1

Veille Technologique

Eliot GIRAUD

Sommaire

Qui ?

Oiltanking

Shell

Société de logistique

Fondée en 1972

Gère 47 terminaux dans 21 pays

Collabores avec Shell

OU et QUAND ?

- Samedi 29 Janvier 2022
- Hambourg (Hamburg) en Allemagne

PAR QUI et POURQUOI ?

Un gang de cybercriminalité lié à la Russie nommé "Black Cat".

Pour obtenir une rançon

QUOI / COMMENT ?

- Le ransomware "Black Cat" (ou **ALPHV** pour les plus fins d'entre vous).

- Aucune communication concernant la démarche des attaquants.

Un peu plus sur "Black Cat"

- Gang actif depuis novembre 2021
- Louent leurs services
- Apparemment lié au gang de ransomware DarkSide, selon un analyste des menaces à la société (Brett Callow).
- Ciblait un large éventail d’industries, notamment la construction et l’ingiénierie, la vente au détail, les transports...

CONSÉQUENCES

Fonctionnent **avec une** capacité **limitée (perte de** chiffre d'affaire)

Déclarer un cas de force majeure (**décrédibilisation** auprès **des** consommateurs **et des collaborateurs)**

RÉACTIONS / SOLUTIONS

- Mènent une enquête approfondie en collaboration avec des spécialistes externes et collaborent étroitement avec les autorités compétentes.
- Ont porté plainte
- Population tenue informée des avancées de l'enquête.

SOURCES

- D'où je suis parti:

https://www.zdnet.fr/actualites/en-allemagne-un-fournisseur-de-carburant-paralyse-par-une-cyberattaque-39936661.htm

- 1er rapport consulté (Anglais) (moins intéressent) :

https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/

- 2nd rapport consulté (Anglais) où j'ai trouvé le rapport initial:

https://thestack.technology/oiltanking-cyber-attack/

- Rapport initial (Allemand):

https://www.handelsblatt.com/unternehmen/energieversorgung-cyberangriff-legt-oiltanking-tanklager-deutschlandweit-vollstaendig-lahm-tankwagen-beladung-ausser-betrieb/28023918.html

- Source sur Black Cat la plus intéressante selon moi pour tout type d'information :

https://alharak.org/attaque-de-ransomware-en-allemagne-liee-a-des-pirates-de-pipelines-coloniaux/