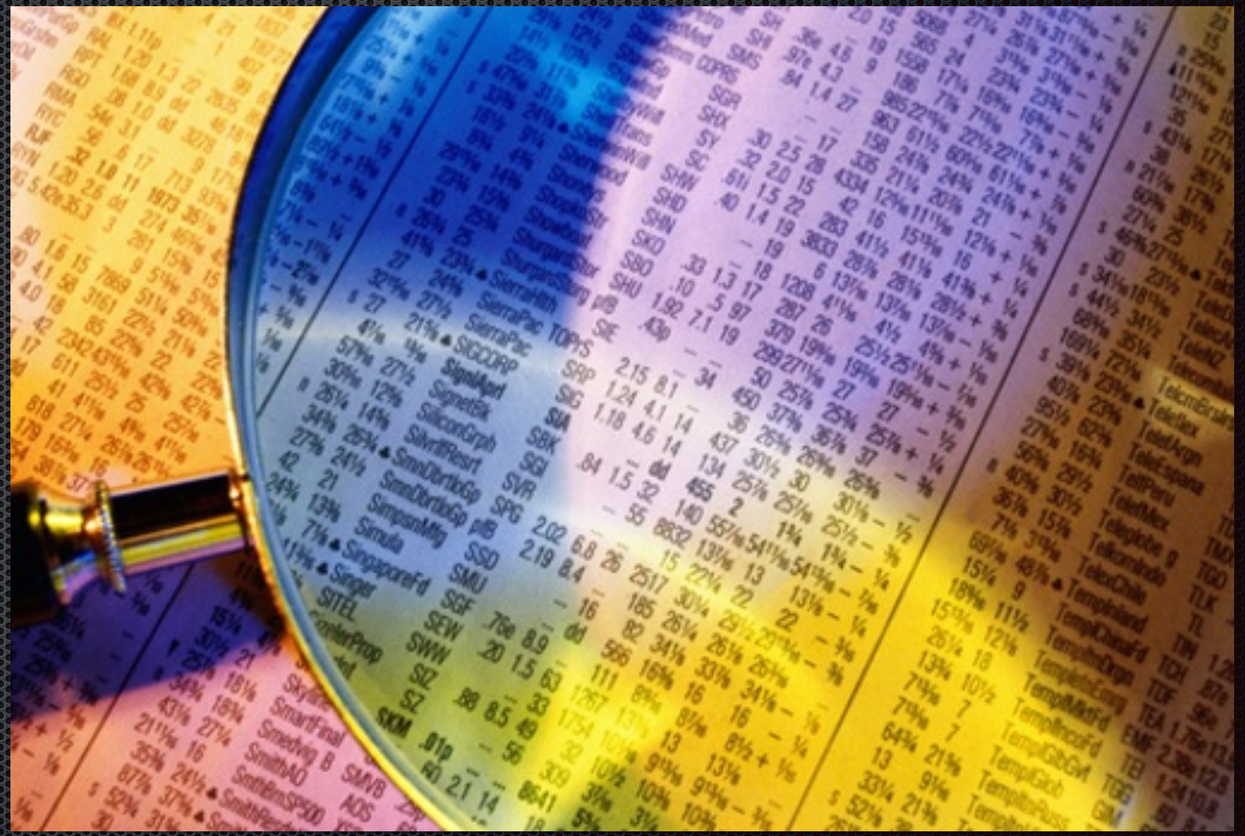
Caso práctico: Recopilación de evidencias

- Nuestra organización ha sufrido un ataque pishing…
- Ha tenido éxito y ha comprometido las credenciales de usuarios
- Usando estas credenciales, y devido a varias vulnerabilidades, los atacantes han escalado privilegios.
- Desconocemos los datos que han podido comprometerse



Para comentar:

- Suponiendo que el ataque ha sido repelido, o eso creemos…
- ¿ que evidencias recopilar? ¿Como? ¿Donde? ¿cuando?
- ¿Que harramienats utilizar?
- ¿Como garantizar una cadena de custodia?