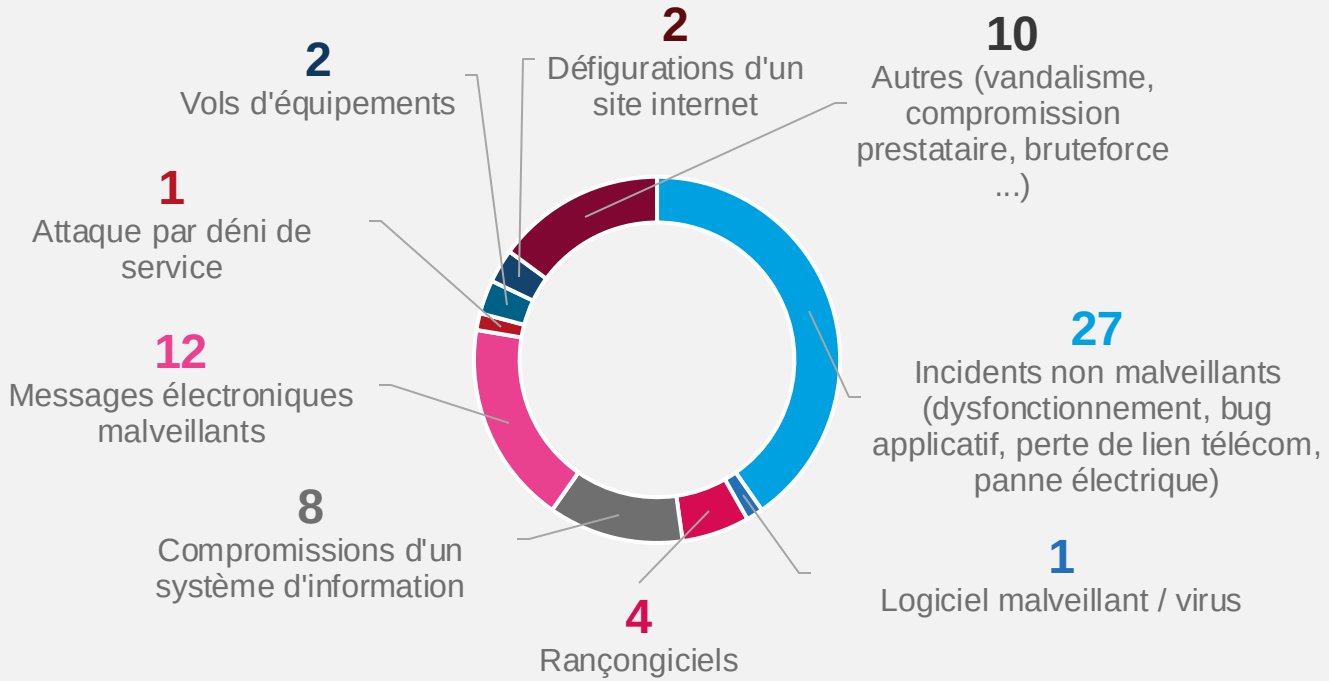
CERT Santé

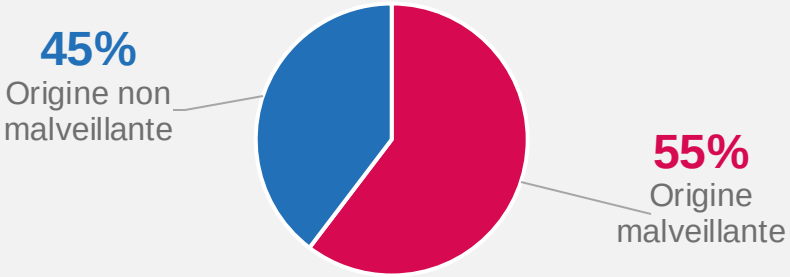
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

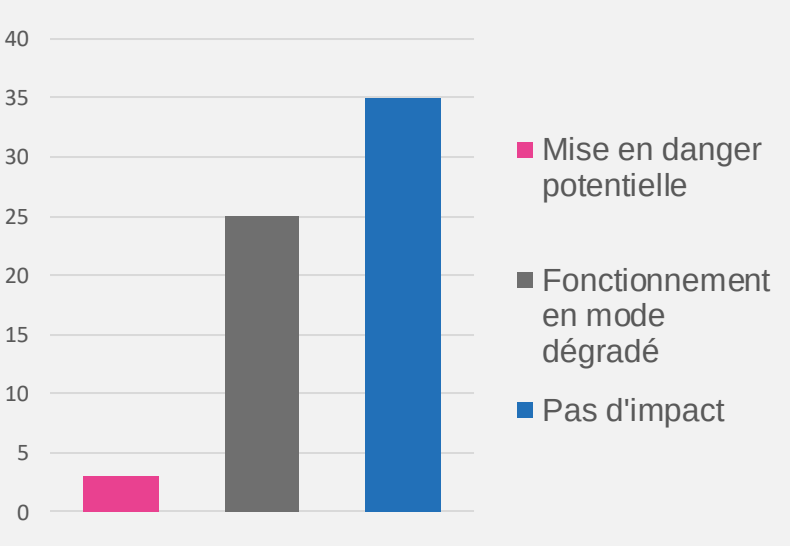
Indicateur sur l'origine des incidents déclarés pour le mois de décembre

Février 2025

Origine des incidents déclarés – Janvier 2025







Origine des incidents déclarés – Janvier 2024

Messages malveillants, compromission du SI et rançongiciel

- Comptes de messagerie compromis via des messages d'hameçonnage, des messages contenant une charge malveillante
- Défiguration d'un site web suite à l'exploitation d'une vulnérabilité pour déployer un webshell permettant de générer des pages écrites en japonais
- Attaque par le rançongiciel RansomHub entrainant la paralysie complète du SI ainsi qu'une perte des données d'un serveur (comptabilité) suite au chiffrement de l'ensemble des serveurs du SI
- Compromission d'un compte VPN entrainant une exfiltration du contenu de l'Active Directory
- Attaque par rançongiciel du Waiting Ransomware Group suite à la compromission potentiel d'un accès RDP ouvert sur Internet entrainant le chiffrement de plusieurs serveurs (serveur Windows / VM / NAS de sauvegarde) et bases de données critiques

Origine des incidents déclarés – Janvier 2024

Logiciel malveillant / virus

Infection d'un poste par le ver Raspberrry Robin suite à l'introduction d'une clé USB entrainant la perte des données stockées sur le poste