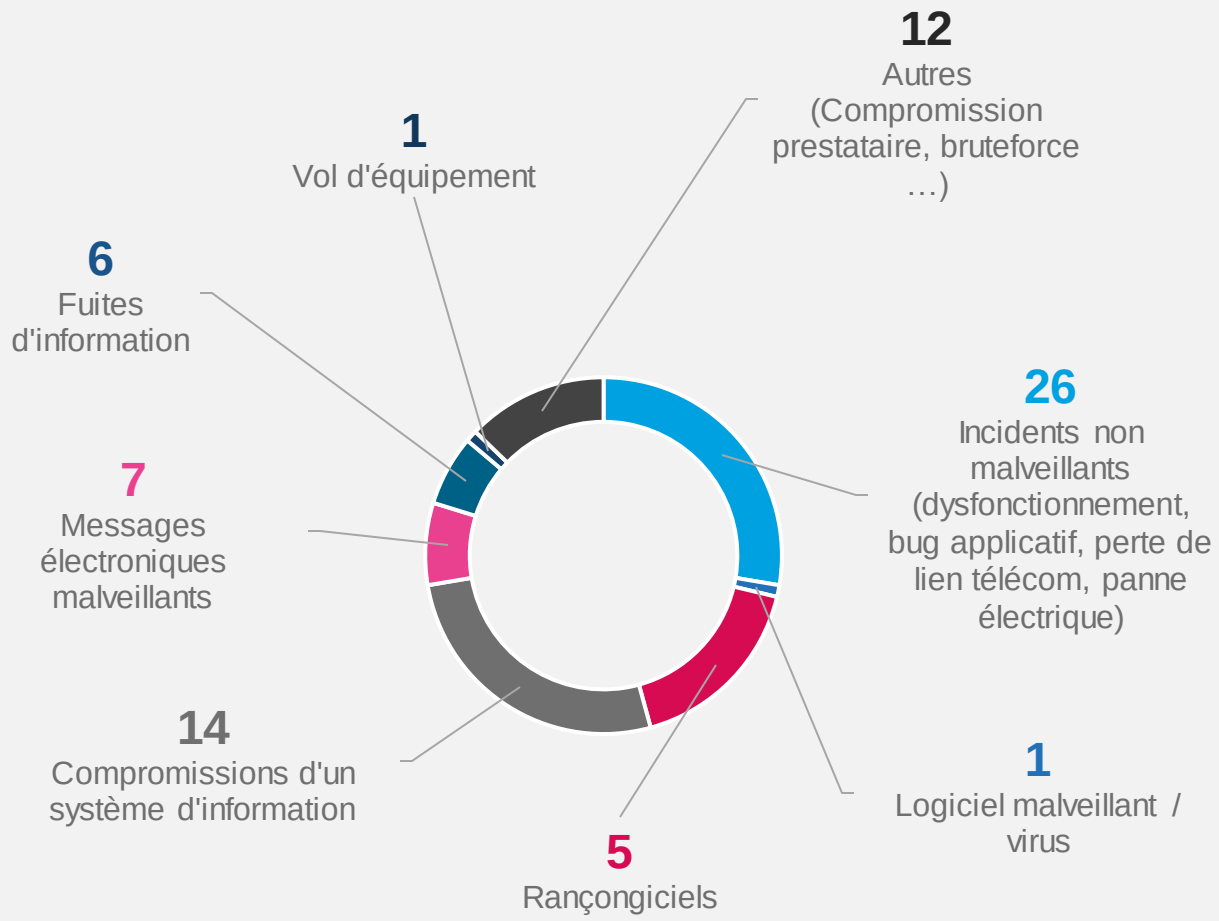
AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

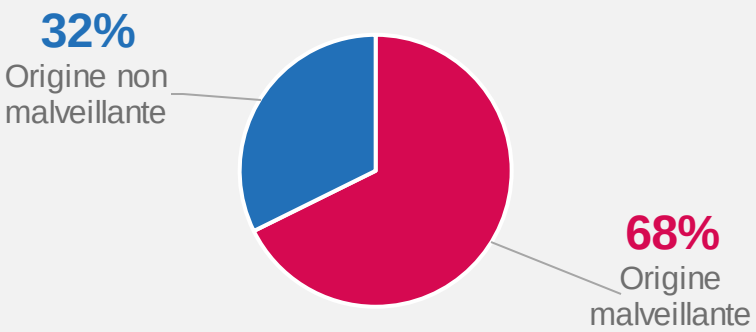
Indicateur mensuel sur l'origine des incidents déclarés

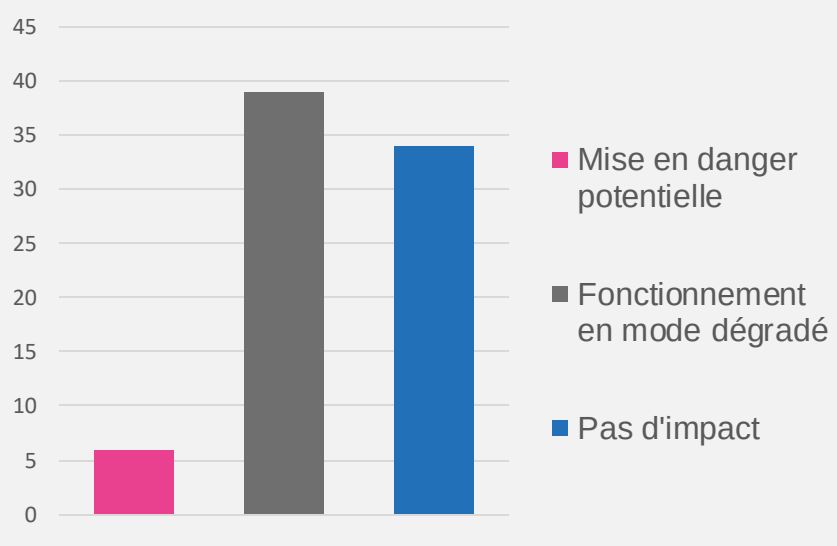
CERT Santé

Mars 2024

Origine des incidents déclarés – Février 2024







Origine des incidents déclarés – Février 2024

Message malveillants, compromission d'un système d'information et rançongiciel.

Comptes de messagerie et postes utilisateurs compromis via des messages d'hameçonnage ou contenant une charge malveillante

Compromission du système d'information par l'exploitation de vulnérabilités **CVE-2024-21762 et CVE-2024-23113** concernant les accès VPN **Fortinet**

Attaque par le rançongiciel **BlackByte** suite à la compromission d'un compte AD par force brute provoquant le chiffrement d'un serveur de sauvegarde et la perte d'accès DPI

Attaque par le rançongiciel **Lockbit** suite à la compromission d'un compte d'accès VPN provoquant une interruption du SI et une fuite de données

Origine des incidents déclarés – Février 2024

Rançongiciels et logiciels malveillants

Attaques par les rançongiciels **RansomHouse (variant Mario)** et **Dharma** (2 incidents distincts) impactant chacun une seule machine. L'investigation n'a pas permis d'identifier la compromission initiale.

Infection d'un poste de travail via une clé USB contenant un logiciel malveillant de la famille **PlugX RAT**. Le logiciel malveillant a été détecté, le poste infecté a été isolé.