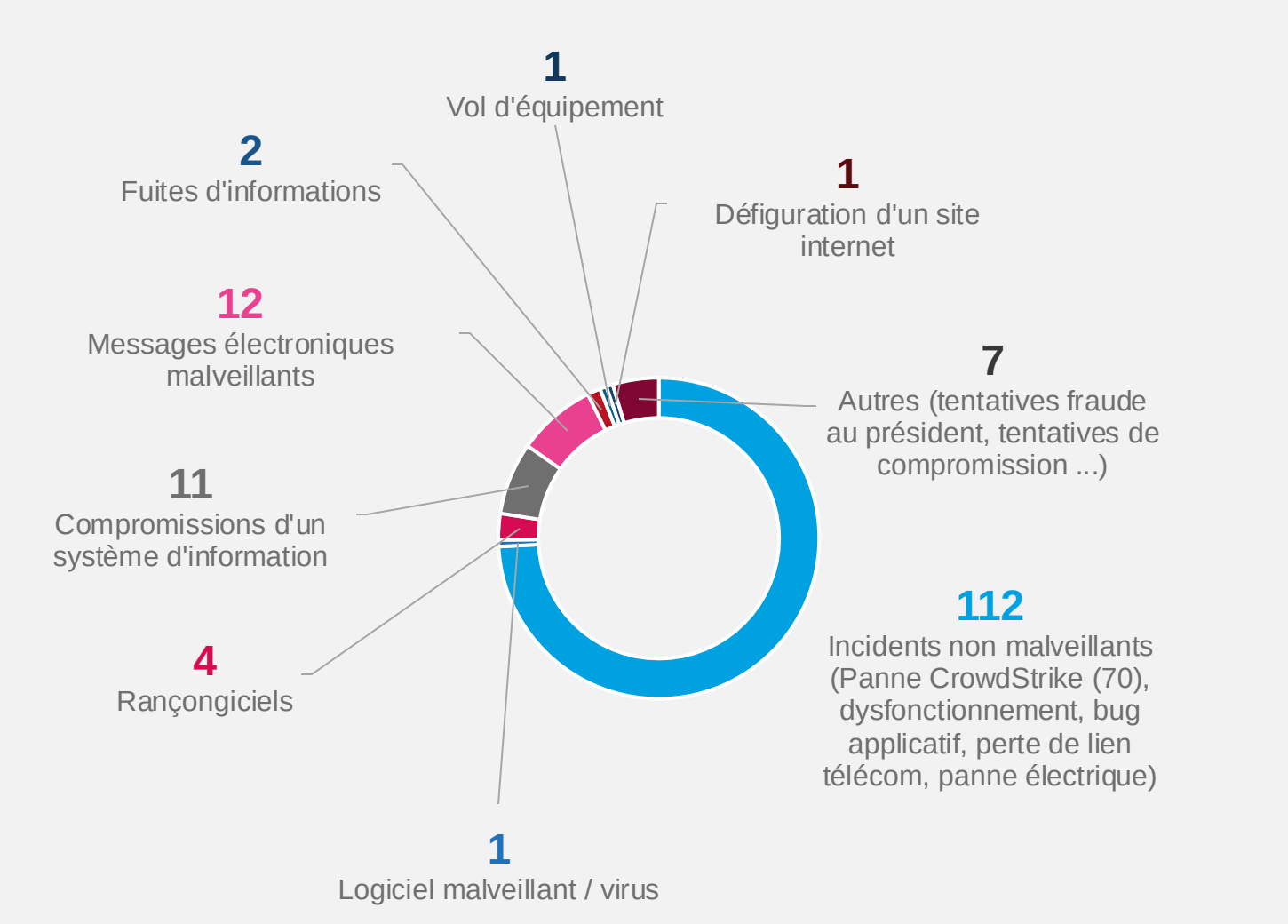
AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

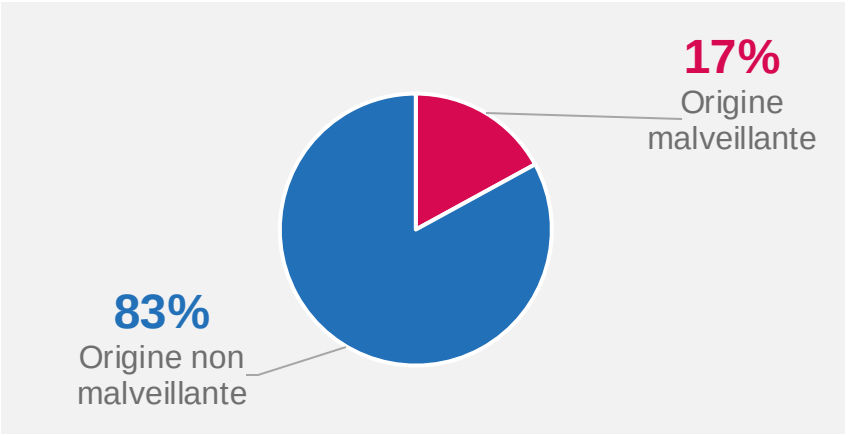
Indicateur mensuel sur l'origine des incidents déclarés

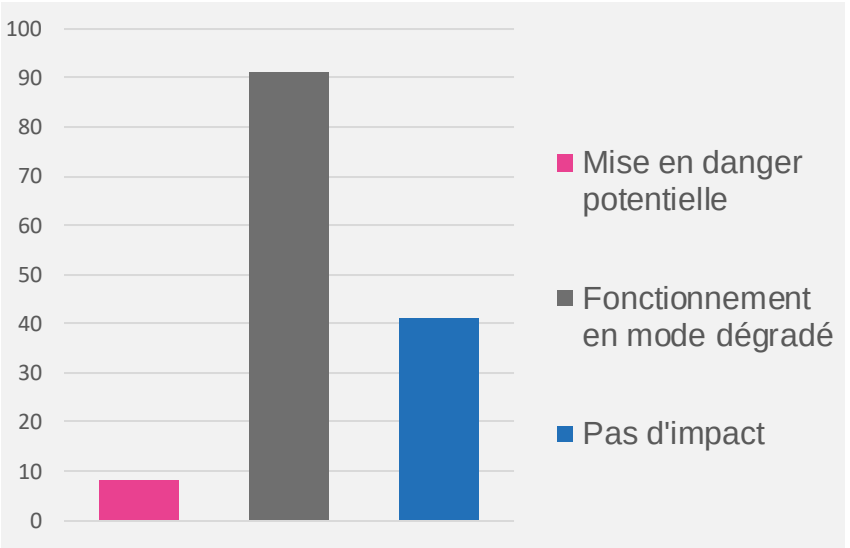
CERT Santé

Août 2024

Origine des incidents déclarés – Juillet 2024







Origine des incidents déclarés – Juillet 2024

Message malveillants, compromission de comptes et rançongiciel

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

Attaque par rançongiciel suite à la compromission d'un compte utilisateur sur l'accès VPN SSL entrainant le chiffrement de disques en réseau

Attaque par le rançongiciel **Makop** suite à la compromission d'un compte d'accès à distance entrainant le chiffrement de fichiers

Attaque par le rançongiciel **Phobos (ELBIE)** suite à la compromission d'un accès de télémaintenance Teamviewer puis d'un accès admin sur le serveur DC entrainant le chiffrement de l'AD et d'un serveur applicatif

Attaque par le rançongiciel **Dispossessor (**dépôt d'une note de rançon) suite à la compromission d'un compte VPN; la découverte d'un mot de passe faible d'un compte admin domaine en clair dans un fichier a permis à l'attaquant de se connecter au contrôleur de domaine. Des données ont été exfiltrées puis les données du serveur ont été chiffrées.

Origine des incidents déclarés – Juillet 2024

Logiciel malveillant / virus

Cryptovirus ayant chiffré l'intégralité des fichiers du serveur infecté ainsi qu'un poste utilisateur avec l' extension ".id[7E2C51C2-2803]"