Le monde de la cybercriminalité ne cesse de prendre de l'ampleur et le paysage des cybermenaces évolue rapidement. Une étude a indiqué qu'à l'échelle mondiale, **40% d'attaques de plus** sont menées par semaine contre les organisations en 2021, par rapport à 2020.

article du «Journal du net» du 04/11/2021

Qu'est ce qu'une cybermenace:

Les cybermenaces sont des tentatives malveillantes destinées à perturber un système informatique ou un réseau en volant des données ou en accédant à des fichiers non autorisés. Les cybermenaces touchent aussi bien les particuliers que les entreprises. Elles peuvent être une source de chantage (ransomware), de monétisation (revente d'infos personnelles sur le dark web), ou d'usurpation d'identité (phishing, etc.) Il est donc recommandé de protéger ses appareils et ses données avec une solution de sécurité.

Les différents types de cybermenace :

- **La cybercriminalité** comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations
- **Les cyberattaques** impliquent souvent la collecte d'informations pour des raisons politiques
- **Le cyberterrorisme** vise à saper les systèmes électroniques pour entraîner panique ou peur

Nos ordinateurs sont controlés:

- par des malwares (logiciels malveillants), ils en existent de nombreux comme : les virus, le cheval de troie, spyware, ransomware, etc.
- le phishing ou hameçonnage : des communications frauduleuses qui semblent provenir d'une source fiable
- les attaques par déni de service (ddos)
- l'injection SQL (Structured Query Language)
- les attaques 0 day
- la tunnellisation DNS

Certains secteurs sont plus touchés que d'autres :

- Les services médicaux,
- les revendeurs au détail
- les entités publiques

sources : Kaspersky - Eset