**Menaces avancées persistantes - Synthèse**

Une **menace avancée persistante** (APT) est un ensemble de processus permettant le piratage permanent et furtif d’un ordinateur, souvent orchestrés par une ou plusieurs personnes à l’encontre d’une entité spécifique. L’APT visera en général soit des organisations privées, soit des Etats, pour des motifs à la fois lucratifs et politiques. Les processus d’APT nécessitent d’opérer pendant très longtemps dans la clandestinité. On parle de processus « avancé » lorsqu’on utilise des techniques sophistiquées reposant sur des maliciels (malware) pour exploiter des vulnérabilités dans des systèmes informatiques. L’APT est « persistante » en ce qu’elle passe par un système externe de commande et contrôle qui, en permanence, surveille une cible spécifique et en extrait des données. Il s’agit d’une « menace » parce que c’est un être humain qui orchestre l’attaque.

On parlera en général d’APT pour un groupe, par exemple un gouvernement, ayant à la fois la capacité et l’intention de viser, de manière persistante et efficace, une entité donnée. L'expression est communément utilisée pour les cyber-menaces, en particulier la menace de l’espionnage au moyen d’Internet grâce à toute une série de techniques de recueil de renseignement pour accéder à des informations sensibles ; l’expression s’applique aussi à d’autres menaces telles que celles de l’espionnage ou des attaques traditionnelles. Parmi les autres vecteurs d’attaques bien connus, on citera les médias infectés, la chaine d’approvisionnement compromise et la technique de « social engineering ».

Ces attaques ont pour but de placer un code malveillant sur un ou plusieurs ordinateurs afin d’y réaliser des tâches spécifiques et d’y demeurer non-détecté le plus longtemps possible. Un professionnel qui connaît les signes laissés par l’attaquant, par exemple les noms de fichiers, pourra plus facilement lancer une recherche sur tout le réseau pour repérer tous les systèmes touchés. On ne parlera pas d’ATP pour un individu agissant seul, par exemple un hacker, qui n’aura que rarement les ressources nécessaires pour mener une attaque à la fois avancée et persistante, même s’il a l’intention d’accéder ou d’attaquer une cible spécifique.

*Source: https://en.wikipedia.org/wiki/Advanced\_persistent\_threat*