**Resumo de Ameaça Persistente Avançada**

Uma **ameaça persistente avançada (APT)** é um conjunto de processos furtivos e contínuos efetuados por *hackers* informáticos, frequentemente orquestrados por uma pessoa ou por várias pessoas que visam atingir uma entidade específica. Uma APT geralmente tem como alvo organizações privadas, Estados ou ambos, por motivos comerciais ou políticos. Os processos APT exigem um alto grau de cobertura durante um longo período de tempo. O processo "avançado" significa técnicas sofisticadas que utilizam *malware* para explorar vulnerabilidades nos sistemas. O processo "persistente" sugere que um sistema de comando e controlo externo esteja continuamente a monitorizar e extrair dados de um alvo específico. O processo de "ameaça" indica o envolvimento humano na orquestração do ataque.

A APT geralmente refere-se a um grupo, por exemplo um Governo, com a capacidade e a intenção de atingir, de forma persistente e eficaz, uma entidade específica. O termo é comummente utilizado para se referir a ameaças cibernéticas, em particular a da ciber espionagem, ativada pela Internet, utilizando uma variedade de técnicas de recolha de informações para aceder a informações confidenciais. Mas aplica-se igualmente a outras ameaças, como a tradicional e clássica espionagem ou ataques informáticos.Outros vetores de ataque reconhecidos incluem meios infetados, comprometimento da cadeia de suprimentos e engenharia social.

O objetivo destes ataques é colocar código malicioso personalizado num ou vários computadores, com o propósito de desenvolver tarefas específicas e de permanecer indetetável pelo período de tempo mais longo possível. Conhecer os artefactos do invasor, como nomes de ficheiros, pode ajudar um profissional a fazer uma pesquisa em toda a rede para reunir todos os sistemas afetados. Indivíduos isolados, como por exemplo um *hacker* individual, geralmente não são considerados agentes de APT, pois raramente têm recursos para serem avançados e persistentes, mesmo que tenham a intenção de obter acesso ou atacar um alvo específico.

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