**Advanced Persistent Threat Summary**

An **advanced persistent threat** is a set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity. An APT usually targets either private organizations, states or both for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "threat" process indicates human involvement in orchestrating the attack.

APT usually refers to a group, such as a government, with both the capability and the intent to target, persistently and effectively, a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attacks.Other recognized attack vectors include infected media, supply chain compromise, and social engineering.

The purpose of these attacks is to place custom malicious code on one or multiple computers for specific tasks and to remain undetected for the longest possible period. Knowing the attacker artifacts, such as file names, can help a professional make a network-wide search to gather all affected systems. Individuals, such as an individual hacker, are not usually referred to as an APT, as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

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