ملخص عن التهديد المستمر والمتقدم (ATP)

التهديد المستمر **و**المتقدم **هو مجموعة من عمليات القرصنة الخفية والمستمرة، ينسقها عادة شخص أو مجموعة من الأشخاص يستهدفون كيانًا محددًا. وعادة ما يستهدف التهديد المستمر والمتقدم (APT) منظمات خاصة، أو دولا أو كليهما بدوافع تجارية أو سياسية. وتتطلب عمليات التهديد المستمر المتقدم درجة عالية من السرية على مدى فترة طويلة من الزمن. ويشير مصطلح "المتقدم" إلى تقنيات معقدة تستخدم برمجيات خبيثة لاستغلال نقاط الضعف في الأنظمة. بينما يشير مصطلح "المستمر" إلى أن نظامًا خارجيًا للتحكم والقيادة يقوم باستمرار بمراقبة واستخراج البيانات من هدف معين. ويشير مصطلح "التهديد" إلى المشاركة البشرية في تنظيم الهجوم.**

**عادة ما يشير التهديد المستمر المتقدم إلى مجموعة، من قبيل الحكومة، ذات القدرة والنية على استهداف كيان معين بشكل مستمر وفعال. ويستخدم هذا المصطلح عادة للإشارة إلى التهديدات الإلكترونية، خاصةً التجسس الممكن عبر الإنترنت باستخدام مجموعة متنوعة من تقنيات جمع المعلومات الاستخبارية للنفاذ إلى معلومات حساسة، ولكنه ينطبق بنفس الطريقة على تهديدات أخرى مثل التجسس التقليدي أو الهجمات التقليدية. وتشمل موجهات الهجمات المعروفة الأخرى الوسائط المصابة بالفيروسات، وسلسلة التوريد العرضة للشبهات، والهندسة الاجتماعية.**

**ويتلخص الغرض من هذه الهجمات في وضع شفرة خبيثة مخصصة على جهاز كمبيوتر واحد أو عدة أجهزة كمبيوتر حتى تنجز مهام محددة وتظل غير مكشوفة لأطول فترة ممكنة. يمكن أن تساعد معرفة الخدع التي يستخدمها القرصان، من قبيل أسماء الملفات، الأشخاص المحترفين في إجراء بحث واسع على مستوى الشبكة لجمع كافة الأنظمة المتأثرة. ولا يشار عادةً إلى الأفراد، من قبيل القراصنة الأفراد، على أنهم مرتكبو التهديد المستمر والمتقدم، حيث نادراً ما تتوفر لديهم الموارد الضرورية لتشكيل تهديد متقدم ومستمر حتى وإن كانوا عازمين على النفاذ إلى هدف محدد أو الهجوم عليه.**

**المصدر: (باللغة الإنجليزية)** [*https://en.wikipedia.org/wiki/Advanced\_persistent\_threat*](https://en.wikipedia.org/wiki/Advanced_persistent_threat)