APT (Advanced Persistent Threat)

APT（高□持久性威□，Advanced Persistent Threat）是指一種高度專業化、有組織結構且持續性的攻擊，通常由國家級的駭客組織、間諜機構或犯罪團體發起。APT攻擊的目標通常是政府機構、軍事機構、大型企業、關鍵基礎設施或其他具有戰略價值的目標。

以下是APT攻擊的一些特點：

1. **高度專業化：** APT攻擊者通常具有高度專業化的技能，能夠使用先進的攻擊工具和技術。他們可能有深入的安全知識，並且能夠使用自定義的惡意軟件。

2. **有組織結構：** APT攻擊通常是有組織結構的，攻擊者之間分工合作，利用不同的技能和專業領域。這可能包括駭客、情報分析師、惡意軟件開發者等。

3. **持久性：** APT攻擊往往是長期的，攻擊者通常會努力保持對受害者系統的持久訪問權。他們可能會悄悄地滲透受害者網絡，長時間觀察和收集數據，而不被發現。

4. **隱匿性：** APT攻擊者通常會使用高度隱匿的技術，以避免被檢測和追踪。這可能包括使用加密通信、定期更改攻擊方法，以及避免觸發安全防禦機制。

5. **有組織目標：** APT攻擊的目標通常是對某個組織的信息、知識產權、商業機密或政府機密進行竊取。攻擊者可能追求長期的情報收集，以支援政治、經濟或軍事目的。

6. **社會工程：** APT攻擊者可能使用社會工程技巧，針對特定目標進行精心策劃的釣魚攻擊，以引誘受害者執行惡意操作。

防禦APT攻擊需要綜合的安全措施，包括強化網絡防禦、實施嚴格的身份驗證和授權措施、定期的安全審查、執行行為分析等。企業和組織也應該保持高度警覺，及時發現並應對潛在的APT攻擊。

修訂版本 #2
★由 treeman 建立於 10 ?Q?G?? 2023 11:28:27
✎由 treeman 更新於 10 ?Q?G?? 2023 11:29:15