進階持續性滲透擊(APT)簡介

進階持續性滲透攻擊(Advanced Persistent Threat, APT)，Advanced 意指精心策畫的進階攻擊手法，Persistent 則是長期、持續性的潛伏。APT 攻擊重點在於低調且緩慢，利用各種複雜的工具與手法，逐步掌握目標的人、事、物，不動聲色地竊取其鎖定的資料。所以能發動這種 APT 攻擊手法的駭客，都是以長期滲透特定組織為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。

根據營運創新資安委員會所提出的策略白皮書中，將 APT 歸納出五種典型的特色：

1. 高度針對性。
2. 具有潛伏並保持低調的技術能力。
3. 擁有資料情報分析之能力。
4. 擁有多樣工具的多重面向攻擊方式。
5. 資金充裕。

因此，能發動這種 APT 攻擊手法的駭客，都是以長期滲透特定組織為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。

APT 與一般駭客攻擊之間的差異如下表：

	APT	一般駭客攻擊
時間	長時間攻擊	長短不一定
動機	竊取所需要的特定機密，包含國家安全、商業機密等	動機不一定，從彰顯自己能力到竊取個資以換取實質利益皆有
攻擊者	有組織、計畫性的團體	一般的個人或駭客結盟
攻擊對象	有針對性、小範圍，如政府、高科技公司、金融業等	無針對性、大範圍，近年以具有大量個人資料的企業為主
攻擊手法	長期、持續性、多樣化，經常是零時差漏洞的攻擊，確保達成攻擊目的	多為速戰速決，複合多種常見漏洞，以大量、快速、有效的單一手法入侵

最後，為了避免遭受到 APT 攻擊，分別有以下幾點法則可以遵守：

1. 人是最後防線，資訊安全的教育訓練是必要的。
2. 關鍵在於如何提供便利的介面給特定人士即時自動詳細檢查可疑文件本身，包括文件標頭、格式、內容，而非延遲至有其他受到駭客攻擊的人或樣本實驗室有特徵碼才能有所因應。

3. 防毒和防火牆確實仍屬必要的防護，但並不足以阻擋現代化的惡意程式和進階資料竊取攻擊。
4. 如果要阻擋 APT 攻擊的話，目前資訊安全防護設備要隨 APT 之攻擊手法進步，持續收集與分析。

資料來源：

[1]. http://adsl.hinet.net/adsl/news_detail.jsp?url_a=news/soc_detail2.jsp?MSG_ID=HSC2011100700001&product_no=
[2]. Xecure Lab - 從 APT 攻擊看全球危機與台灣轉機
[3]. http://blog.xecure-lab.com/
[4]. http://www.websense.com/assets/reports/state-of-security-infographic.pdf