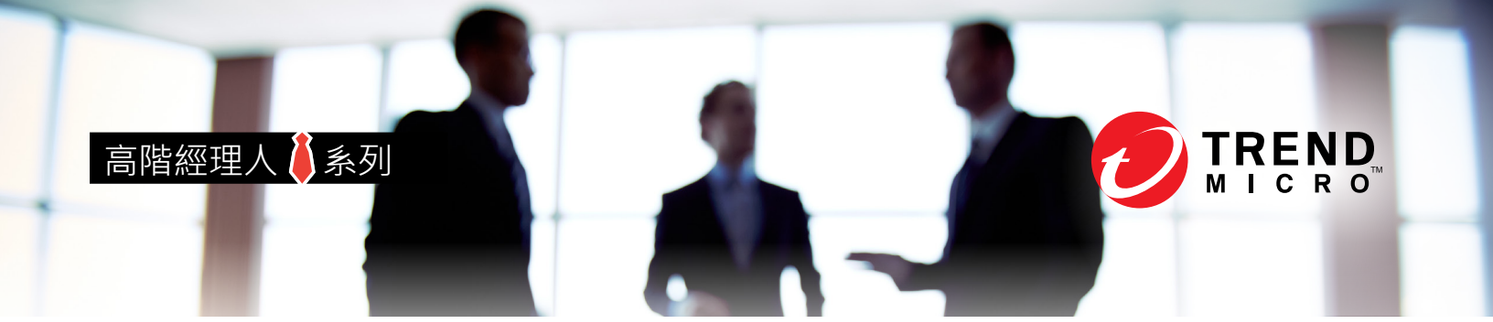

漏洞攻擊服務

網路犯罪服務系列

網路犯罪服務 (Cybercrime as a service，簡稱 CaaS) 是深層網路 (Deep Web) 論壇上的一項重要發展，它讓更多不法之徒能夠輕易取得網路犯罪的工具和服務，如此一來，就連不具技術背景者都只需花點小錢就能從事網路犯罪。不僅如此，網路犯罪集團也開始發現，將攻擊目標從家用使用者擴大到企業網路可以帶來莫大好處。針對這一點，IT 系統管理應該做好心理準備。

漏洞攻擊套件

網路犯罪地下網路第一次出現的漏洞攻擊套件是 2006 年的 WebAttacker，它收錄了常見 PC 軟體的漏洞，並且提供一整套的基礎架構來方便發動攻擊[1]。不過，有別於一些較制式的商品，如個人身分識別資訊 (PII)，漏洞攻擊套件通常在網路論壇而非網路市集上販賣[2]。

如同在真正開放的市場一樣，網路犯罪開發人員很快就發現，專業分工可以帶來更高的效率和利潤。駭客只需專心做好網路犯罪基礎架構，其他的人就可以在這基礎上進行一些自動化和客製化。

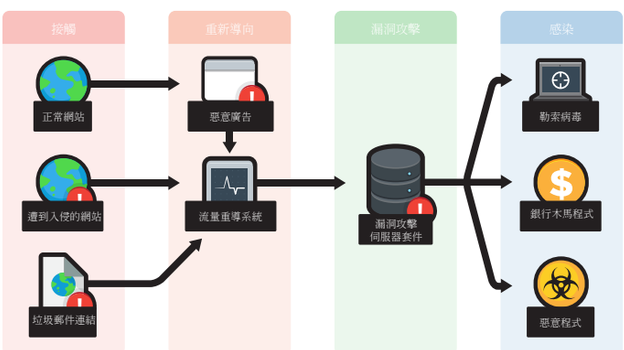

圖 1：典型的漏洞攻擊套件攻擊流程[3]

惡意程式攻擊行動當中讓非專業人士很難入門的一點就是，如何開發和執行漏洞攻擊，而這卻是網路犯罪集團取得龐大獲利的關鍵，因為這種攻擊方式的成功率很高。藉由攻擊漏洞，歹徒就不需仰賴使用者來點選某個連結或檔案就能感染系統，因為這類攻擊通常是利用軟體的漏洞來執行惡意程式碼。也因此，漏洞攻擊成了順道下載 (drive-by download)、惡意廣告、水坑式攻擊，甚至是更陰險狡詐的針對性攻擊的重要元素。

> 在 2014 年當中有超過 **100 個漏洞**
> 被收錄到 70 個漏洞攻擊套件當中。

當某個軟體漏洞在網路上流傳並被歹徒用於攻擊時，廠商通常會釋出修補程式來解決該問題。因此，若有一種網路犯罪服務能夠保證漏洞攻擊一定成功，並且可以涵蓋最多的新漏洞，甚至涵蓋當時最新的系統漏洞，那就能賣得好價錢。今日的漏洞攻擊套件已經包含了這樣的服務，甚至可以按小時計費出租，而駭客則專門負責開發漏洞攻擊和提供代管伺服器。

> 漏洞攻擊套件可採租用方式，按小時、日、月計算。當 Angler 漏洞攻擊套件開始走下坡時，Neutrino 的價格立即漲了一倍，
> **從每個月 3,500 美元調升至 7,000 美元**[4]。

「漏洞攻擊套件 + 勒索病毒」的強力組合

目前最流行也最可怕的惡意程式類型，就是能夠讓歹徒挾持系統上的檔案來向使用者勒索贖金的勒索病毒 (Ransomware)。

2015 年，Angler 漏洞攻擊套件開始散布勒索病毒。隨著網路犯罪營運的每一個環節都日益壯大，未來將有更多使用者面臨勒索病毒的恐懼。

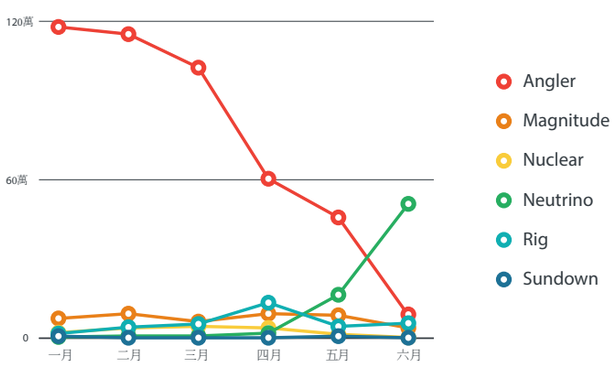

圖 2：2016 上半年專門散布漏洞攻擊套件的網址存取次數。

這些年來，漏洞攻擊套件多如過江之鯽，但真正成功者通常都是那些能夠迅速收錄最新漏洞、並且具備各種躲避偵測技巧者。

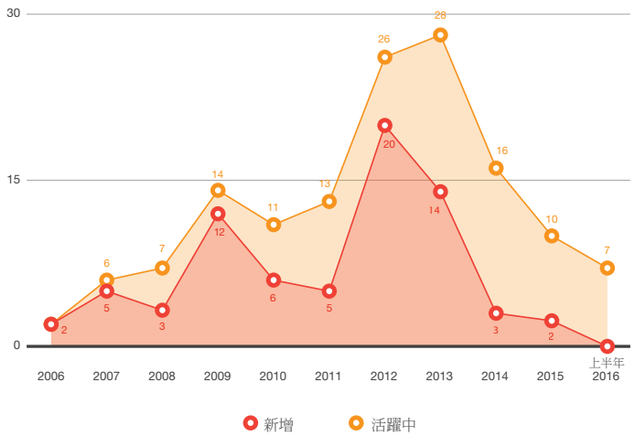

圖 3：2006 年至 2016 上半年新增與活躍中的漏洞攻擊套件。

這對企業的意義為何

光是 2016 上半年，趨勢科技 (加上 TippingPoint) 和 ZDI 漏洞懸賞計劃就發現和/或揭露了 473 個漏洞[4]。漏洞數量最多的是 Adobe® Flash® Player，這是今日系統上相當普遍的一套軟體。

Adobe Flash 是漏洞攻擊套件的頭號目標，目前有超過10 億台連網系統皆普遍裝有這套軟體。

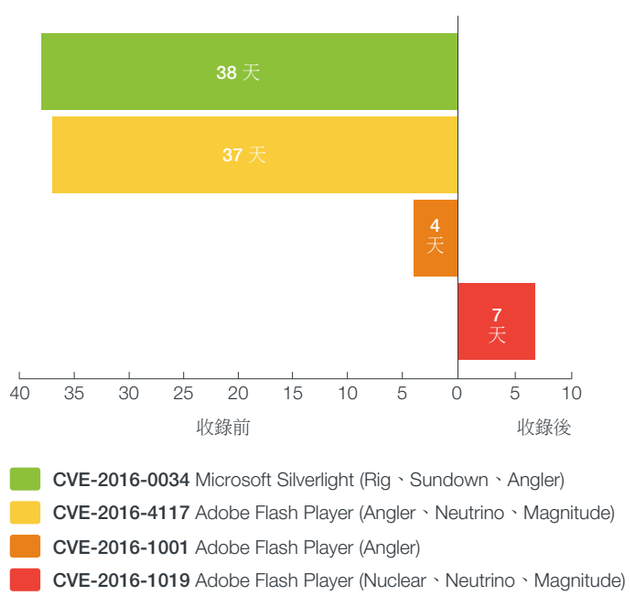

圖 4：2016 上半年漏洞攻擊套件收錄漏洞的空窗期。

由於零時差漏洞很快就會被收錄到漏洞攻擊套件當中，因此資安廠商與駭客之間有如一場貓追老鼠的競賽，在這樣的情況下，企業的網路隨時都可能遭遇到威脅。

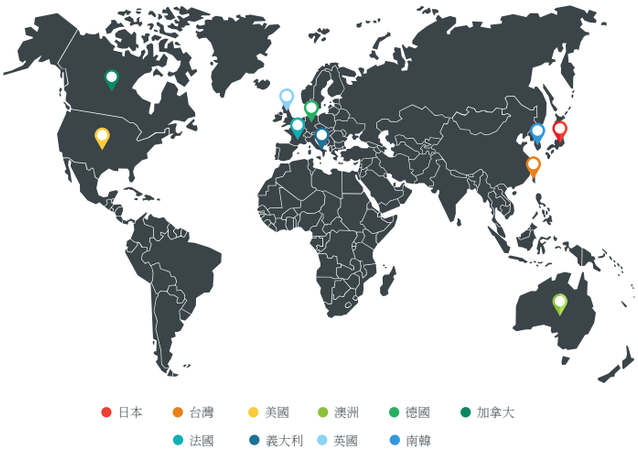

圖 5：2016 年第二季所有點選漏洞攻擊套件相關連結的使用者有 80% 都來自這十個國家。

只要網路犯罪集團繼續運用「漏洞攻擊套件 + 勒索病毒」這樣的致命組合，企業就必須小心應付勒索病毒感染的風險，以及任何惡意程式與漏洞攻擊套件經營者可能發展出來的新點子。

漏洞攻擊套件	散布的勒索病毒	
	2015 年	2016 年
Angler	CRILOCK (CryptoLocker)	CRILOCK (CryptoLocker)
	CRYPTESLA (TeslaCrypt)	CRYPTESLA (TeslaCrypt)
	CRYPWALL (CryptoWall)	CRYPWALL (CryptoWall)
		WALTRIX (CryptXXX)
Neutrino	CRYPTESLA (TeslaCrypt)	CERBER
	CRYPWALL (CryptoWall)	CRYPTESLA (TeslaCrypt)
		CRYPWALL (CryptoWall)
		LOCKY
		WALTRIX (CryptXXX)
Magnitude	CRYPWALL (CryptoWall)	CERBER
		CRYPWALL (CryptoWall)
Rig	CRYPTESLA (TeslaCrypt)	CERBER
	CRYPWALL (CryptoWall)	GOOPIC
Nuclear	CRYPCTB (Cryptroni/ Critroni/CTB-Locker/ Curve-Tor-Bitcoin Locker	CRYPTESLA (TeslaCrypt)
	CRYPSHED (Troldesh)	LOCKY
	CRYPTESLA (TeslaCrypt)	
	CRYPWALL (CryptoWall)	
Sundown		CRYPTOSHOCKER
Hunter		LOCKY
Fiesta	CRYPTESLA (TeslaCrypt)	

表 1：各漏洞攻擊套件所散布的勒索病毒。

在勒索病毒事件當中，資料損失是立即的風險，除此之外還有一些其他直接和間接的後續效應，都將影響企業的生計，包括：

- 業務損失
- 付款、交貨或交易延遲
- 訂單無法出貨
- 業務流程中斷
- 生產力損失
- 法律賠償
- 政府罰鍰
- 品牌及商譽損失

企業能做些什麼

能夠修補的漏洞應該盡快修補，不論是資料庫應用程式或者是瀏覽器附加元件。這是網路防禦的基本原則，並且應該被視為一項關鍵的資安工作。

然而，為了維持營運，企業不允許系統為了進行修補而隨意停機。此外，某些老舊、內部自行開發或廠商不再支援的軟體，可能再也無法進行修補。因此，採用入侵防護 (IPS) 過濾規則來暫時防堵端點上的漏洞，是企業退而求其次的最佳選擇。

今日的資料中心混合了實體、虛擬和雲端平台，因此企業的資安策略應該要能具備適應能力，並且要能從單一主控台進行控管。

趨勢科技深知完整分析整個攻擊流程——從入侵點 (如惡意網址和垃圾郵件) 以及漏洞攻擊套件和各種躲避偵測技巧的運用，到回報給幕後操縱的歹徒——以及強化惡意程式攔截能力，不讓它們有機會在系統上執行的重要性[6、7]。

隨著網路防禦的規模擴大到數千個需要保護的端點，不同的防護層之間必須要能「彼此互相溝通」以形成一個環環相扣的威脅防禦策略。所有的防護層都必須能夠取得資安技術所能提供的最新威脅情報、安全更新及防護，例如：

- 進階的惡意程式防護 (不單只有黑名單)
- 在網站及訊息閘道上的垃圾郵件防護
- 網站信譽評等
- 應用程式控管 (白名單)
- 內容過濾
- 漏洞防堵
- 行動應用程式信譽評等
- 入侵防護
- 主機式防火牆防護

只要前述各項技術能夠合作無間，就能偵測今日絕大多數的威脅。但是，新的軟體漏洞還是會不斷被發現，廠商只能盡快加以修補。因此，企業最終還是得要藉由行為與系統一致性監控以及沙盒模擬分析之類的技術，來具備偵測零時差「未知」威脅的能力。

尤其，機器學習技術可藉由不斷學習人工或電腦所輸入的範例來歸納出一套數學模型，進而偵測漏洞攻擊套件的活動。藉由「訓練」資安產品，網路防護就能即時防範那些難以偵測的威脅，例如漏洞攻擊套件。

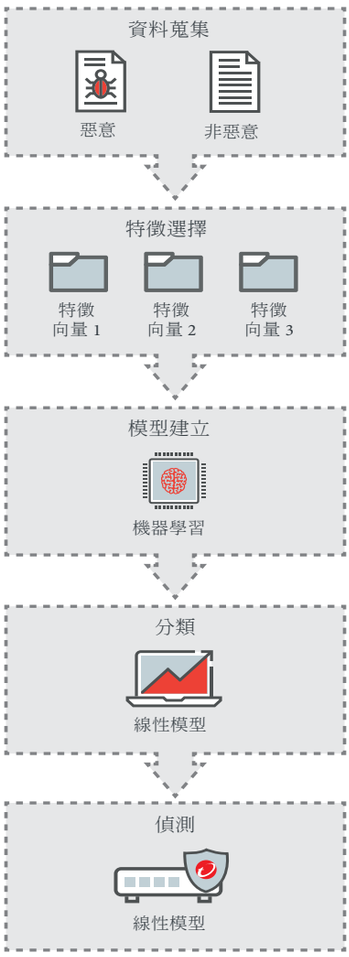

圖 6：機器學習如何防範漏洞攻擊套件。

參考資料

[1] https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-evolution-of-exploit-kits.pdf

[2] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/wp-russian-underground-2.0.pdf

[3] http://www.trendmicro.com/vinfo/us/security/definition/Exploit-Kit

[4] http://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

[5] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-the-reign-of-ransomware.pdf

[6] http://www.trendmicro.com/us/enterprise/product-security/vulnerability-protection/

[7] http://www.trendmicro.com/us/business/network-security/

©2016 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。本文件之內容若有變動，恕不另行通知。