白皮書

Fortinet 先進威脅防護 (ATP) 架構

解決進階持續性滲透攻擊(APT)之緊密防護方式

Fortinet 先進威脅防護架構

目錄

NetFOS 逸盈科技 www.netfos.com.tw

台 北
台北市八德路四段760號7樓
TEL: +886 2 6636-8889
FAX: +886 2 6638-9998

新 竹
新竹縣竹北市高鐵二路32號13樓之5
TEL: +886 3 621-5128
FAX: +886 3 668-4058

台 中
台中市文心路四段696號7樓之2
TEL: +886 4 3606-8999
FAX: +886 4 3602-0999

高 雄
高雄市裕誠路392號10樓之2
TEL: +886 7 862-8889
FAX: +886 7 862-9998

介紹

為重大報酬所設計的複雜而精巧之攻擊

我們在2013與2014兩年都能看到許多重要品牌與大公司登上了報紙的頭條，不過那並不是因為它們在景氣衰退之後有重大的財務復甦或者是推出了什麼創新產品，而是因為發生了大量的資料外洩。超過一億名客戶的個人與/或信用卡資料就在這些大膽且後續影響深遠的攻擊事件中遭竊。

這些攻擊事件引起了消費者、政府與媒體的注意，因為它們成功侵入的是非常大的組織，而這些組織還都擁有專屬的安全團隊以及專門設計用來抵擋駭客入侵的基礎軟硬體設備。事實上，就連小型組織也無可避免，無論是大型協同攻擊中的一部分，或者是透過各式各樣四處流傳的惡意程式所攻擊或入侵；只要存在利益，就是攻擊目標。

看來無人可以免疫的發酵議題背後我們所該關心的是什麼？尋找更深入且更全面之網路安全解決方案的時候到了。

「所有組織現在都應該要假設他們正持續受到來自網路的攻擊。」

- *Gartner*

「2014年一項調查指出，有18%的組織通報被外部人士成功地侵入它們的內部網路。」

- *PwC*

「接受調查的組織中，有44%企業表示資料外洩是它們執行NGFW專案的最主要原因。」

- *Forrester / Fortinet*

欺騙是駭客軍火庫中最強大的工具

受到資料駭入成功的激勵，我們預期會看到網路罪犯間持續不斷的創新，而且進一步將重點放在欺騙與迴避現有的安全解決方案。帶著惡意的駭客經常利用各種檔案形式與壓縮檔案來嘗試隱藏惡意程式，其用意就是要利用傳統網路防護方式的弱點。我們也預期能針對鎖定攻擊進行客製化之精密惡意程式平台的數量將會有所增加。

一旦惡意程式侵入了一個網路，該程式就會自動或在網路罪犯的控制下以躲避偵測的方式盡可能地變形、適應和移動，並且採集從客戶資料記錄及情資財產權到裝置設定檔案與員工密碼等各種資料。**如果安全監控機制在這段期間無法偵測到惡意程式或其通訊，那麼收集到的資料會流出，也就是被傳送到網路罪犯手上就只是遲早的事。**

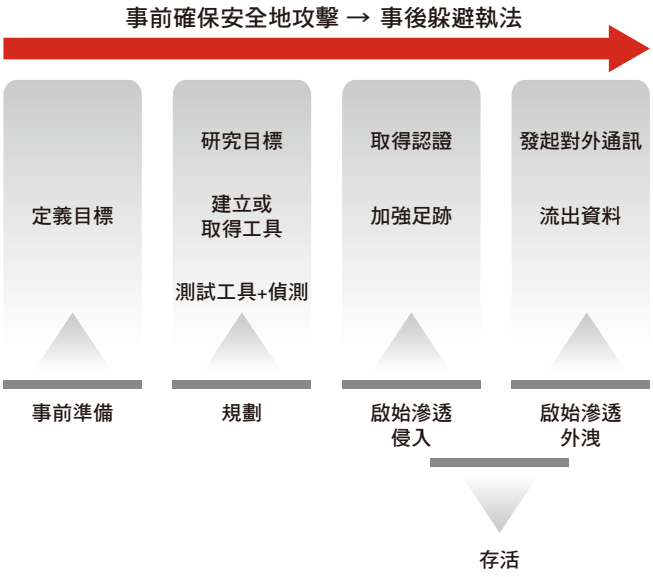

圖1：APT攻擊的詳細步驟

對抗APT攻擊需要先進威脅防護

沒有一種「金鐘罩」能夠完全保護組織不受上述各種先進鎖定目標式攻擊的威脅。惡意程式一方的快速創新、頻繁的零時差(zero-day)攻擊以及新興的躲避技術都可以讓任何單一的防護方法失去效果。

反而最有效的防禦是建立在緊密且可延伸的防護架構上。這種架構整合了最新的資安防護能力、新興技術以及根據最新偵測到的威脅產生具有即時資安防護力的自動化學習機制。這也讓使用者能夠自始維持超前於威脅曲線之最重要的一部份。

解決複雜威脅的簡單架構

Fortinet先進威脅防護架構包含三大要素：

- **預防**—針對已知威脅與資訊行動
- **偵測**—找出先前未知的威脅
- **緩解**—回應潛在可能發生的事件

這個架構的概念非常簡單；其中包含有各式各樣先進與傳統的網路、應用程式、終端保全、威脅偵測與緩解方式等工具。這些工具都具備強大的研究與威脅情資能力，可將多種來源之威脅情資轉換成具行動力之資安防護。儘管架構裡的要素(甚至其中的科技)都可以獨立運作，但如果這些要素同時被當作全方位保全策略的一部分一起使用時，組織將可以達到更堅固的防護。

要素1—預防 針對已知威脅與資訊行動

針對已知的資安威脅應立即利用次世代防火牆、安全電子郵件閘道、終端保全以及可以充分利用高精密保全科技的類似解決方案直接阻絕(Fortinet先進威脅防護架構中的要素1)。這是**以對網路效能影響最小的方式擋掉多種威脅的最有效率方法。**

例如防惡意程式的科技可以運用Fortinet專利的緊密模式辨認語言(Compact Pattern Recognition Language, CPRL)等技術，以最小的處理時間來偵測並阻擋病毒、殭屍網路甚至預測的惡意程式變形。
我們也可以藉由減少可攻擊的層面和範圍來嚇阻攻擊。網路罪犯可以運用的侵入點或潛在威脅點越少越好，也就是說，小心管制存取權限與執行VPN會是要素1的一大重點，並且也是鎖定目標攻擊防禦前線的一部份。

而那些無法迅速處理的流量就交給要素2…

要素2—偵測
找出先前未知的威脅

要素1已解決許多威脅並建立防護，其顯著優點是，落入已知類別的威脅越多，愈適合使用。然而，駭客最愛使用未知的「零時差」威脅與設計可以躲過傳統措施的精密攻擊來滲透高價值的目標。這時，就需要建立起架構中的**要素2，採用先進威脅偵測科技來更仔細的檢查網路流量行為、使用者與內容以找出新的攻擊手法。**
有一些新的方法可以自動偵測先前未知的威脅並建立具行動力的威脅情資。目前最好的方式就是沙箱處理(Sandboxing)，透過沙箱可以將潛在的惡意軟體傳遞給有掩蔽的環境，這樣就可以直接觀察其行為而不致影響使用中的線上網路。此外，殭屍網路偵測功能可以標示出顯示有殭屍網路活動的通訊模式，而客戶的聲譽分析（Client Reputation）可根據使用者相關的流量分析(Contextual Profile)標示出潛在受感染的端點。
這種威脅偵測方式雖然功能強大，不過相當耗費資源，也因此最好是用來處理無法以更有效率之傳統方式確認的威脅。當然偵測只是ATP架構的另一項要素而已。下一個要素就會以決定性方式解決這些新威脅。

要素3—緩解
回應潛在可能發生的事件

一旦要素2確認潛在的事件與新威脅時，組織就立即需要驗證威脅並減輕任何損害。
使用者、裝置與/或內容應該要隔離，而且要有自動與手動系統來確保網路資源與組織資料的安全性，直到確保網路恢復安全狀態為止。
在此同時，威脅偵測會觸發另一項關鍵的後續作業—將發現的威脅資訊回傳到研發團隊。先前未知的威脅此時就可以被深入分析，產生出可以整合入所有保全層級的修補方式並提供每一個層級最新的防護組合方式。在此階段，使不同保全科技之間建立協同綜效成為部署高效能防護方案，並使未知威脅變成已知威脅。

當這項具行動力之威脅情資可以全面性分享，同時要素1也能夠強固到可阻擋新的已知威脅，此時才真正的完成完整的防禦週期(如下圖)。如此不但可以幫一個組織，也可以協助全球各地的組織抵擋網路罪犯。

以最有效率的方式(結合1、2、3三個要素)執行偵測與預防對於維持高層次網路效能與防護最大化而言至關重要。

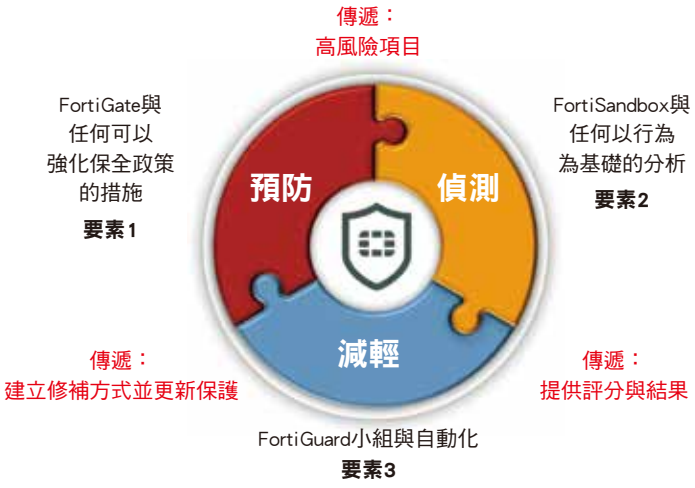

圖2：Fortinet先進威脅防護架構

傳遞—遺落的環節

威脅防護架構中最需要的關鍵能力—同時也是許多組織的保全措施中所沒有的—就是傳遞(Handoff)。

先進威脅防護依靠的是多種資安技術、產品與研究，各自身負不同的角色。不過這些項目彼此之間若不能持續做溝通並將資料在彼此之間傳遞，那麼各自之間的效果就無法彰顯。

如圖2所示，預防階段的要素1會將高風險項目傳遞給偵測階段的要素2，而先前未知的威脅會傳遞給要素3進行後續的分析或緩解。最後要素3所產生的威脅情資與防護更新就會往回傳遞到要素1與2，因此這個**持續的週期就可有效率地改進對不斷增加之精密攻擊所提供的防護與偵測**。

Fortinet幫助您走在威脅曲線的前面

FortiGuard實驗室綜效與研究

Fortinet最大的強項之一就是其專屬軟體、高效能設備與最重要地FortiGuard實驗室威脅研究小組之間所產生的綜效。FortiGuard實驗室研究小組的功用就像可以確保三大要素緊密合作的情報中心。各小組會研究先前未知的威脅，開發以高效能與高效率防護為基礎之完善補救策略，並提供可以持續隨時間強化預防與偵測的保全情資。

完善的保全：FortiGuard實驗室充分利用威脅地貌的即時情資在各種Fortinet解決方案與核心科技之間傳遞完整的資安更新資訊以達到綜效的防護。

領先威脅一步的防護：當新的威脅浮現時，FortiGuard實驗室的7x24小時全年無休全球作業會將最新的保全情資即時送到Fortinet解決方案，達成新興威脅的立即防護。

高效能解決方案：Fortinet的整合安全服務是從頭開始設計以便在所有的Fortinet安全解決方案上—實體與虛擬雲端—達到防護最大化與效能最佳化。

當FortiGuard實驗室所開發的廣泛威脅情資透過全球Fortinet分配網路（FDN）傳送到所有Fortinet解決方案使用者手上時，要素3就會傳遞到要素1與2，其中就會完成例行性的先進威脅防護循環週期。此外，身為網路威脅聯盟(Cyber Threat Alliance)與其他相關計畫的一份子，Fortinet也會與大量的研究人員分享威脅情資，並進一步擴展其工作以及在此架構下所發現之組織產生威脅情資所能及之範圍。

Fortinet解決方案共同提供更好的防護

有很多個別的安全產品雖然很強大，不過要是單獨作業時就無法達成最佳的安全性。解決方案中的每一個部分都需要共同合作才能提供最佳化的防護。Fortinet將FortiGuard實驗室的情資整合到FortiGate次世代防火牆、FortiMail安全電子郵件閘道、FortiClient終端保全、FortiSandbox先進威脅偵測與其生態系統中其他產品以便持續最佳化與改進各組織的安全層級。

如需更多有關Fortinet與其先進威脅防護系列產品各方面的資訊請造訪網站：
www.fortinet.com

FORTINET
Fortinet, Inc. Taiwan
台北市內湖區行愛路176號2樓
TEL:02-27961666
FAX:02-27960999
網址:www.fortinet.com.tw

關於 Fortinet

Fortinet (NASDAQ : FTNT)協助用戶抵禦不斷演進的網路威脅，保護客戶的網路、使用者和資料。身為高效能網路安全的全球領導者，**Fortinet**能讓企業和政府能協同並整合各種單項的資安防護技術，而不必忍受拙劣的效能。和其它昂貴、缺乏彈性和效能低落的其它解決方案不同，**Fortinet**的解決方案能讓客戶在保護重要系統和內容資產的同時，也能擁抱新技術與商業契機。