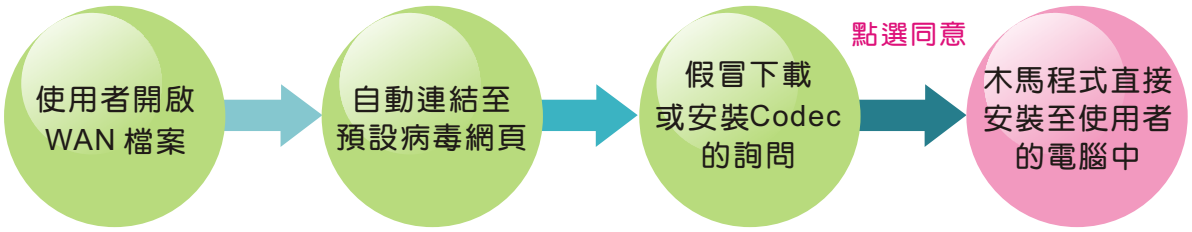
新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2008/11/10- 2008/11/23 第80期

多功能 UTM / MS 系列報導

技術淺談與應用 - MS 該如何防範新型木馬利用 WMA 格式入侵

在網路病毒層出不窮的環境下，為了達到能入侵使用者的電腦，病毒的入侵管道及方式也同樣的不斷在變，然而某知名防毒廠商近期也發現了新的木馬入侵方式。這次則是利用 WMA 影音檔案來當作感染途徑的新型蠕蟲程式，可在使用者電腦安裝木馬病毒，以做為網路罪犯控制。

新品種的蠕蟲會隱藏在 Windows Media Audio（WMA）格式的檔案中，並增入連結至受感染的網頁。一旦使用者開啟檔案，並且連到該網頁，就會開啟一個下載或安裝 Codec 的詢問。如果使用者同意安裝這個檔案，木馬程式將直接安裝至使用者的電腦中，進而成為網路罪犯控制的殭屍電腦。



木馬入侵流程圖

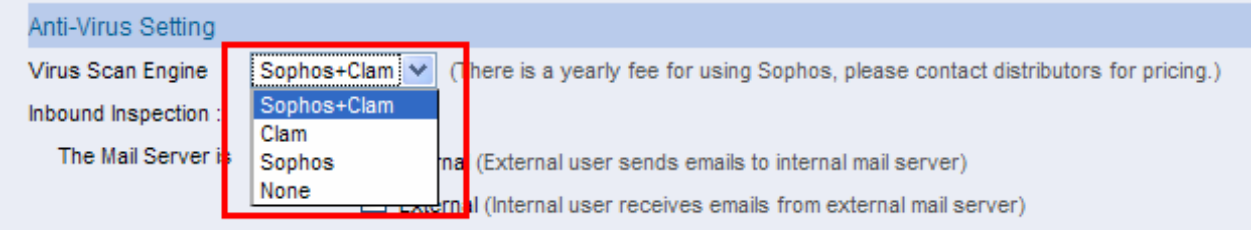
根據知名防毒廠商分析，到目前為止這是第一個屬於感染影音檔案的蠕蟲，也正因為如此，大部分的使用者不認為這些影音檔案可能受到感染，也不曾因此類型檔案而受感染，以致於造成攻擊成功機率不斷的增加。

倘若公司一不小心被此類木馬所入侵，重要文件及機密資料被外洩的機率也就相對的大為增加，為了預防此類新品種病毒、木馬，一般人處理的手法即是立刻更新電腦中所安裝的防毒軟體來做預防，當然不可否認這也是必須的處理動作之一，但往往卻也忽略了此類型屬於新種的病毒，在往後的日子裡也有變種型態出現的極大可能性，而公司何時會被入侵也因此變成了未知數。

員工所使用的是公司內部的電腦而非一般家用電腦，一但出了問題，所連帶造成的損失是無法相比擬的，若是像一般家用電腦只以更新病毒碼來作預防處理的動作，往後所需面臨的風險也相對較高。為了能夠徹底的保護公司網路資訊的安全，“新軟多功能 UTM-MS” 則能夠輕鬆的滿足資安人員的需求。利用多功能 UTM-MS 中管制條例裡的 “Download” 功能來做針對 WMA 格式的管制。如此的設定，一方面可管制公司內部因下載 WMA 影音檔案而佔用頻寬的問題，另一方面則可讓員工減少偷懶摸魚的時間，同時也讓公司大為減少病毒入侵的機率。

功能畫面截圖

而檔案的來源當然絕對不會只是單單經由下載的管道而來，市面上多數的應用程式也都可能成為感染的途徑，為了能夠達到更完善的防護，管理人員同時還可搭配 MS 中“Application Blocking”的功能，再視公司情況而作最適當的控管及輔助，可有效的降低病毒來源的管道及公司內部不必要的頻寬浪費，並且同時配合利用 MS 所內建防毒機制（雙掃毒引擎 ClamAV、Sophos）線上更新病毒碼，還可針對 SMTP、POP3、HTTP、FTP的掃瞄，如此一來即可多方面的防護，使公司內部擁有乾淨的網路環境。



功能畫面截圖

項目	內容	備註
掃毒引擎	ClamAV Sophos	目前已可偵測超過四萬種以上的病毒、蠕蟲以及木馬程式，並 24 小時隨時線上自動更新病毒碼。ClamAV 可永久免費更新病毒碼，而且並無使用人數限制。這可讓病毒防護功能，能以最少的成本，永遠保持在最新的狀態。免受病毒、木馬、惡意網頁程式、間諜軟體、網路釣魚...危害。
支援防護方面	SMTP POP3 HTTP FTP	

病毒偵測功能

文 陳殿鴻 kim@nusoft.com.tw

市場行銷報導 - 讓公司不再有電腦「毒患」的身影

根據統計，台灣上網人口早已經超過一千五百萬人，不過到底有多少人的電腦因為病毒入侵而中毒呢？若以一般的中小企業的情況來統計，一台電腦一年平均要中毒八十六次，相對的公司也必須得要花上高額的維修防護費用，而家庭用戶則是每一百台電腦中，就有三十八台曾經感染電腦病毒，加上木馬、病毒不斷的推陳出新在眼前，台灣有超過七成五的人都在使用病毒電腦。

病毒在網路世界裡，無所不在，而發出電腦病毒網址的來源，百分之三十四點二出自美國，百分之三十點一出自中國大陸，而病毒程式中，百分之三十是在中國寫的，其中又以特洛依木馬型病毒佔大多數，甚至有些病毒還會自我更新，讓人防不勝防，這些病毒幾乎都是利用使用者愛貪小便宜的心態及聳動人心的標題來使用戶踏入陷阱，像是在非法網站下載音樂和影片、瀏覽不明的情色網站、開啟不明的網址和信件…等，這些都極容易讓電腦中毒的使用行為。

在公司裡，有著眾多的部門，部門裡又有不少的員工，而每個員工所使用網路的行為及習慣也都大不相同，面對處於危機四伏的網路環境下，為了避免公司內部電腦因種種的使用行為而導致中毒，管理人員又該如何去一一防範、一一限制內部員工的網路使用行為呢？

對於無法一一去限制公司內員工的網路使用行為，一般處理的手法大多會選擇於前端採購、架設防火牆來做為公司最前線的防護，但倘若單單只使用防火牆的話能力卻也有限，在現階段的網路世界裡，依然是無法阻擋各地蜂湧而來的病毒。而若是於每台電腦上再加裝防毒軟體，每一期所需支付的軟體費用則必然讓老闆大嘆吃不消。為了能有效的將公司裡的電腦做到完善的防護，必須額外採購的安全設備到底需要多少台才夠？

這些讓人頭痛且煩人的問題就交給新軟系統，新軟系統所推出的“多功能 UTM - MS”系列產品將眾多強大的功能整合為一體，公司只需架設一台就可抵多台使用，不需要再為了不同的防護機制而多浪費額外的採購成本，同時產品所內建之重量級防毒機制 - 雙掃毒引擎 ClamAV、Sophos，可針對 SMTP、POP3、HTTP、FTP 加以防護，並且隨時自動線上更新病毒碼，讓防毒的效能永遠保持在最佳的狀態，不用擔心會錯過任何更新病毒碼的時機。

此外 MS 還擁有“應用程式管制”功能，不必擔心員工不當的濫用公司網路，管理人員只要利用管制功能，不但可以輕鬆又準確的限制公司內部員工的網路使用行為，最為重要的是可降低病毒利用各種管道入侵的風險，也能有效的為公司頻寬上減少不必要的浪費。加上 MS 還備有郵件上的各種安全機制及入侵防禦的偵測功能，與內部異常流量的警示功能，以全方面的方式為公司內部打造一個最優質的網路環境，讓公司可省下大量而且不必要的額外開銷。

	新軟多功能UTM	一般市售網路安全設備
採購成本	較低 (功能合一，一台抵多台)	較高 (必須適需求而分項購入多台)
額外支出(電費、維護費用)	低 (只需一台，節能又環保)	高 (多台機器較費電，相對的維護費用自然多)
設備整合相容性	完美整合 (完美整合成一台，完全不用考慮相容性問題)	問題較多 (多台式的架設，相容性較容易有影響)
操作、設定難易度	低 (使用單一介面，操控簡單)	高 (多種介面，不易控制處理)
防毒效能	高 (採用雙掃毒引擎，24 小時隨時線上自動更新病毒碼)	低 (單掃毒引擎，能力有限)

公司採購基本顧慮比較表

	新軟多功能UTM	一般防火牆 及各式安全設備	每台電腦 安裝防毒軟體
架購成本	低(只需一台)	中	高
架設難易度	低	高	高
支援病毒更新	○	×	○
日後維護成本	低	高	高(需不斷的支付使用費用)
控管使用者上網行為	○	×	×
全方面的病毒防護	○	×	×
內部異常流量警示	○	× (需管理人員主動查閱)	×
廣告垃圾及病毒郵件的過濾與阻擋	○	需依功能購入相關防火牆設備	× (過於陽春，不敷使用)

防護功能比較表

除此之外 MS 還有更多的相關機制功能，讓公司在不論是在防護、管理、使用方面都能無往不利，更可以輕鬆的處理內部網路所有大大小小的事，若欲瞭解更多、更詳細的功能及規格歡迎請至：http://www.nusoft.com.tw/

文 陳殿鴻 kim@nusoft.com.tw