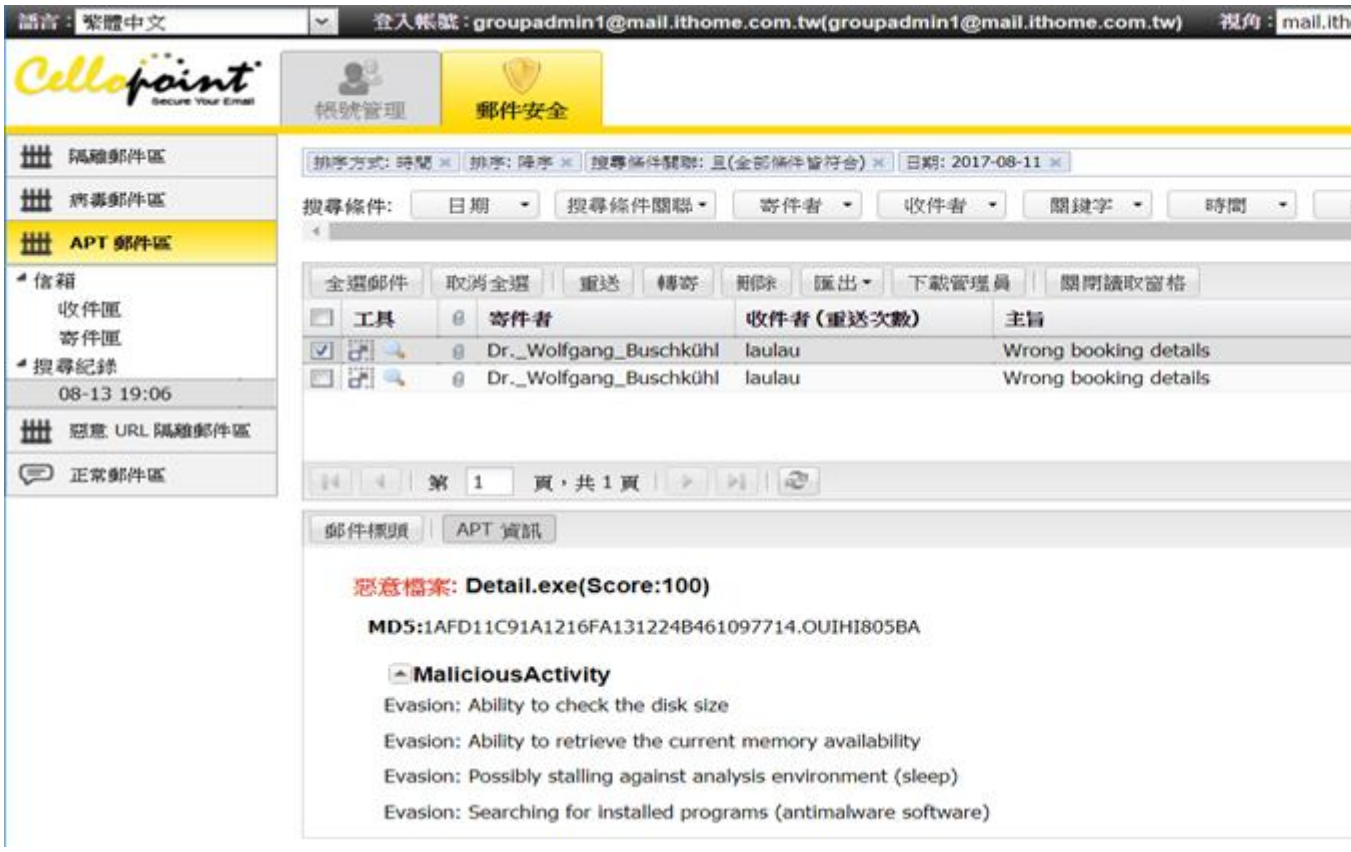
【針對電子郵件與網頁的內容，過濾潛藏的危機 】內容安全是上網防護的核心

勒索軟體的散播管道，也包含電子郵件及網頁，企業需透過內容管理閘道設備，加以偵測與管控

文/周峻佑 | 2017-12-31 發表



在網路流量的過濾之後，企業針對上網的內容，也需要進一步的透視，減少員工經由收發電子郵件、瀏覽網頁等情況下，遭到有心人士下手，發動勒索軟體攻擊的機會。

雖然，現在新的次世代防火牆和 UTM 設備，基本上也具備了檢視網路第 7 層的能力，然而，這類產品仍以流量的初步過濾為主要功能，由於電子郵件是重要的溝通管道，郵件安全性便成為建置防火牆設備之後，企業首要強化保護的目標。另外，由於上網也很有可能遇到內含惡意軟體的網頁，因此網頁瀏覽的安全性，企業同樣要加以保護。

保護郵件安全是當務之急

在公司裡面，員工未必能受允許瀏覽網頁，但幾乎都會使用電子郵件信箱。而對於這種類型的防護措施中，我們這次徵詢相關資安廠商時，有許多國產品牌，都積極回覆產品如何回應勒索軟體攻擊，當中包含了基點資訊、網擎資訊、中華數位，以及趨勢科技等。

在這些品牌的郵件閘道設備裡面，針對勒索軟體威脅的進階偵測，我們看到基點資訊的 Secure Email Gateway，最為突出，在防毒引擎和垃圾信過濾之外，對於疑似 APT 攻擊的惡意軟體和釣魚網址，內

建相關措施，包含網址的黑白名單比對，並與 CelloCloud 結合，運用其中的威脅情資，以及沙箱進階掃描。

而對於進階威脅的偵測，中華數位在他們發展的 Spam SQR，則是能夠將郵件附檔，交由 McAfee Advanced Threat Defense 分析；而趨勢科技的 InterScan Messaging Security Virtual Appliance，能搭配同廠牌的 Deep Discovery Analyzer，共同運作。至於網擎資訊的 MailGates，目前尚未提供沙箱進階檢測機制，但已經著手規畫在 2018 年第 1 季，推出可選購的動態沙箱功能模組。

在國產解決方案之外，還有像是 Forcepoint、Cisco，以及 Fortinet 等外商，也提供電子郵件內容檢測的產品。此外，訴求針對進階持續性攻擊，像是 AhnLab、Cisco、CloudCoffer 、FireEye 系列、Verint，以及趨勢科技的解決方案，同樣可對於電子郵件提供防護。

針對郵件附檔清洗的新興機制

在前述的郵件安全閘道中，由於主要的防護機制，多以垃圾信、掃描附件病毒的方式進行，對於進階威脅的檢測，缺乏像是端點防護的行為分析機制，而是交由沙箱觸發，但許多駭客透過環境偵測機制，迴避這種型態的檢查，勒索軟體一旦發現處於沙箱環境時，就不會發作。

因此，有廠商提供檔案消毒的技術，拆解電子郵件的附件，移除有問題的內容後，再將附件提供給使用者。

目前提供這樣產品的廠商並不多，Opswat 與 Votiro 兩者的解決方案，都有代理商引進，而在檢測電子郵件內容的解決方案之外，也在不同的應用上推出保護措施，像是對於端點電腦的外接式儲存裝置提供軟體，或是以 API 等方式，消毒應用系統收到的檔案。

不過，值得留意的是，這樣的產品能處理的檔案，包含了常見的 Office 文件、圖片、ZIP 壓縮檔案等，並非對於所有檔案類型都適用。而且，這種型態的郵件消毒閘道解決方案，仍是訴求輔助郵件安全閘道的不足，不代表採用後，企業就能完全取代郵件安全閘道。

維護網頁瀏覽安全之餘，也要能解讀使用者上網行為

現在企業的電腦執行許多工作時，都要上網，因此，網頁瀏覽防護也是相當重要的一環。不過，這個領域的國產產品並不多，我們這次詢問到的廠商，僅有利基網路和趨勢科技推出相關設備。

在利基網路推出的網頁安全閘道設備 InstantCheck 當中，而對於偵測進階惡意軟體的沙箱，InstantCheck 設備尚未提供相關措施，但廠商已規畫在 2018 年 2 月，推出 InstantTrace 雲端沙箱服務。

相較於實體設備的 InstantCheck，趨勢科技的 Interscan Web Security Virtual Appliance，則適用於虛擬化環境部署。

至於國外產品的部分，在我們徵詢勒索軟體防護解決方案的過程中，有 Citrix 、McAfee、Forcepoint、Symantec，以及 F5 等公司，表示能夠在網頁安全閘道的部分，提供防護。

而且，除了透過沙箱提供進階分析機制外，也開始有廠商結合使用者行為分析（UEBA）機制，進一步解讀上網行為。像是 Citrix 的 NetScaler Secure Web Gateway ，能搭配使用者上網行為分析系統，進階分析勒索軟體潛入的蹤跡；而若是想要針對使用者的上網行為加以分析，採用 McAfee Web Gateway 的企業也可將網頁安全閘道，連結 McAfee 的 SIEM 平臺 Enterprise Security Manger，取得相關威脅的預警資訊。

勒索軟體網路內容防護產品列表（一）

類型	廠牌	品名	建議售價
郵件安全閘道	基點資訊	SEG-50	10萬元（未稅）
	網擎資訊	MailGates	50人12萬元起
	趨勢科技	InterScan Messaging Security Virtual Appliance	每人1,348元起
郵件APT防護	趨勢科技	Deep Discovery Email Inspector 1000s	1,732,500元起
網頁安全閘道	趨勢科技	Interscan Web Security Virtual Appliance	每人1,303元起
	利基網路	InstantCheck 8000	248萬元起（未稅）（註1）
	McAfee	McAfee Web Gateway	每人4,504元
	Citrix	NetScaler Secure Web Gateway VPX-200	1,467,500元起（未稅）
內容清洗	Opswat（註2）	Metadefender Email Security	每人每年360元（未稅）

註1：包含8000個使用者軟體授權　註2：代理商為達友科技　資料來源：廠商提供，iThome整理，2017年12月

勒索軟體網路流量防護產品列表（二）

類型	廠牌	品名	建議售價
郵件安全閘道	中華數位	Spam SQR	廠商未提供
	Cisco	Email Security Appliance	廠商未提供
	Forcepoint	Forcepoint Email Gateway	廠商未提供
網路APT防護	AhnLab（註1）	Malware Defense System	廠商未提供
	CloudCoffer（註2）	MatrixShield	廠商未提供
	FireEye	EX	廠商未提供
	Verint	Threat Protection System	廠商未提供
網頁安全閘道	F5	Secure Web Gateway Services	廠商未提供
	Forcepoint	Forcepoint Web Gateway	廠商未提供
	Symantec	Secure Web Gateway	廠商未提供
內容清洗	Votiro（註3）	Secure E-mail Gateway	廠商未提供

註1：代理商為瑞奇數碼　註2：代理商為創弘科技　註3：代理商為力悅資訊
資料來源：廠商提供，iThome整理，2017年12月