2013 年網路威脅預測-McAfee

原文出處：MCAFEE (CERT 譯)

http://www.mcafee.com/us/resources/reports/rp-threat-predictions-2013.pdf?ClickID=bmudln6dqemmquvlueqfsqefkf6snfsq6qvs

手持裝置威脅

惡意軟體狂熱購買行為

一旦犯罪者發現有利可圖的技術，他們便會將其重用並且將其自動化，舉例來說，Android/Marketpay.A 是一種木馬程式，會令使用者的手機自動下載需要付費的應用程式而無需使用者的同意。

下載的應用程式中包含惡意軟體開發者所開發的應用程式，藉此讓惡意軟體開發者有一筆可觀的收入，當使用者下載此應用程式時，手持裝置蠕蟲便會透過漏洞滲透在此平台上進行散播，不再需要受害者去安裝此惡意軟體，也就是說，與使用者之間的互動如果是不需要的話，將沒有任何方法能夠防止行動裝置蠕蟲進行狂熱購買的行為。

NFC 蠕蟲

擁有近距離無線通訊功能的手機目前已經越來越普遍，當使用者能夠透過點擊來付費的地方越來越多的時候，他們便會隨時隨地使用電子錢包。但不幸的是這種靈活性也令犯罪者感到興趣，犯罪者創建出含有 NFC 功能的手持裝置蠕蟲透過碰撞並感染的方式來散播與偷取金錢，在人群擁擠的地區透過這種方式對於惡意軟體撰寫者來說，是最容易感染受害者與從他們的電子錢包盜取金錢。

封鎖更新

手持裝置服務提供商在處理惡意軟體的優勢之一為當發現到新的惡意軟體時，便會自動通知使用者更新以便保護使用者的手持裝置。對手持裝置惡意軟體來說，如果要在手持裝置中持續感染很長一段時間的話，就必須防止這些更新，主要藉由下載一個應用程式來封鎖手持裝置與手持裝置服務提供商之間的通訊就可以達到此目標。

惡意軟體

針對 OS X 和手持裝置的惡意軟體套件

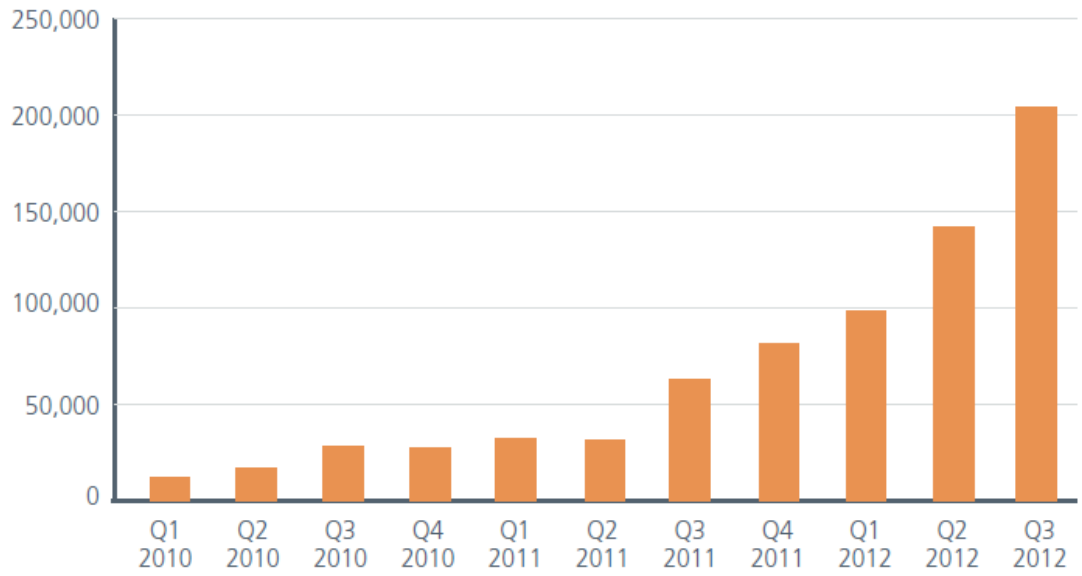
由於手持裝置的普遍，網路犯罪者對此也進行長時間的滲透，在 2012 年，對於移動裝置的威脅數量已大幅上升，當我們對其做更進一步的了解時，我們在地下市場發現到大量以 Windows 為主的攻擊惡意軟體套件。在 2013 年勒索套件率先從惡意軟體套件中出現，我們已看到許多以 OS X 和手持裝置為勒索目標的案例，所以對於以往只能攻擊 Windows 為主的攻擊惡意軟體套件來說，這種情況很快便會有所改變。

勒索軟體持續擴張至手持裝置

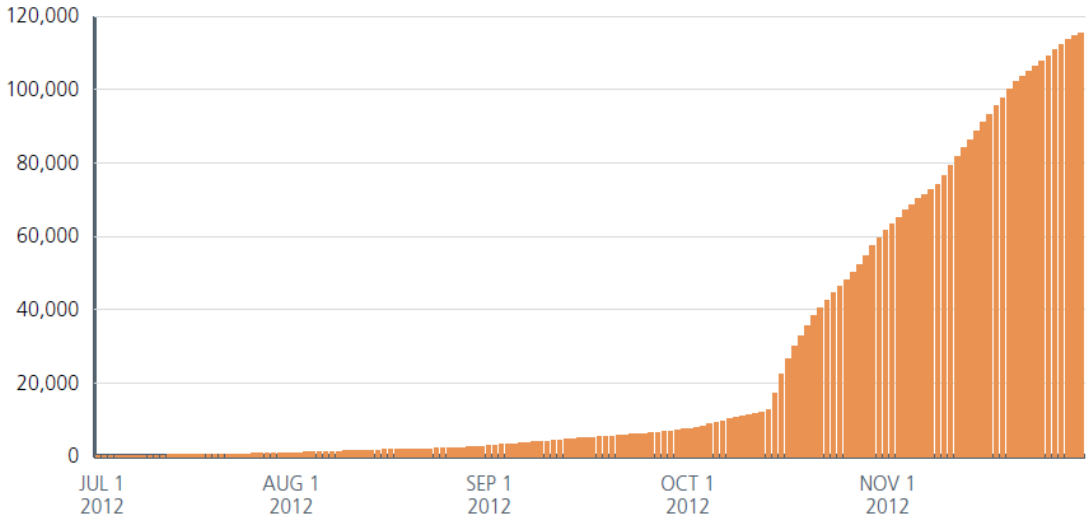
Windows 電腦上的勒索軟體在過去一年來增加了兩倍之多，攻擊者已經證明此種攻擊方式能夠增加他們的利潤，勒索軟體與其他類型的惡意軟體，像是後門程式、鍵盤側錄和密碼盜取等不同的地方在於這些軟體會透過受感染的電腦來進行金融交易，但是勒索軟體則是綁架使用者存取、通訊或使用系統的能力，藉此逼迫他們支付贖金。

透過手持裝置來進行勒索的限制之一在於大部分使用者仍會使用電腦進行交易而不是手持裝置或是筆記型電腦，但是這種情況並不會持續很久，手持裝置的便利性會讓使用者慢慢地將自身業務轉移至手持裝置上，因此攻擊者也已經開始開發手持裝置上的勒索軟體。

我們預計在 2013 年這方面的活動會相當頻繁。



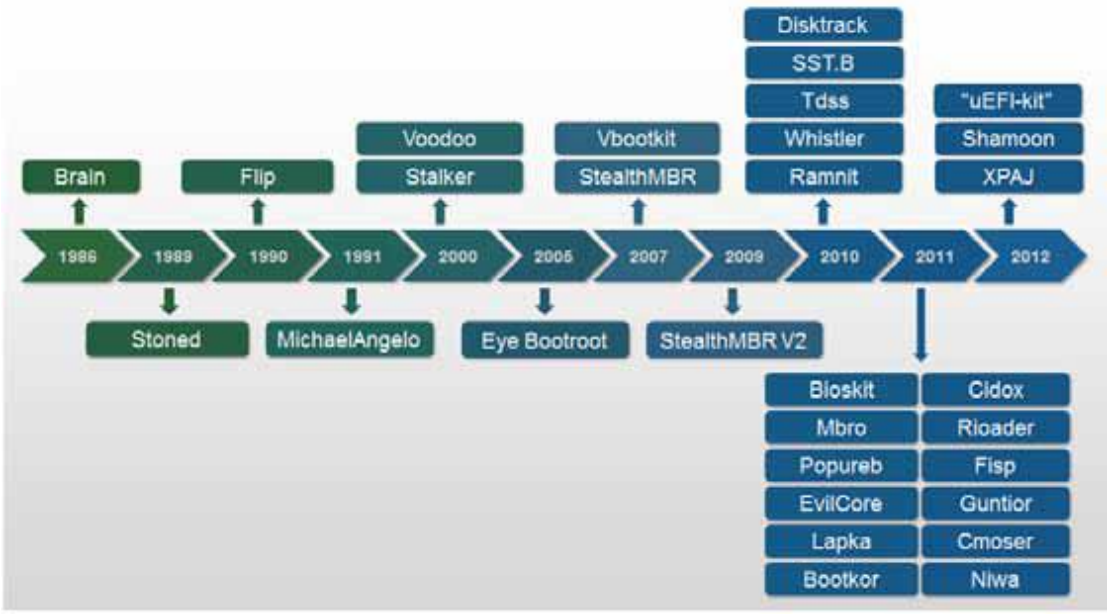
(圖 1)新的勒索軟體樣本



(圖 2)消費者所回報的勒索軟體偵測(累加)

Rootkit 使用 MBR 與其他 bootkit 技術來增加其多樣性

電腦資訊安全軟體和其他客戶端防護的演化驅使了威脅慢慢朝向作業系統不同的區塊，特別是那些隱藏且持續的攻擊。這些攻擊 Microsoft Windows 核心的頻率有增加的趨勢，像是基本輸出輸入系統(BIOS)、主開機磁區記錄(MBR)、裝置開機磁區(VBR)、GUID 磁碟分割表(GPT)和 NTLoader。雖然一般簡單的攻擊對於 Windows 和應用程式來說，並不會構成任何威脅，但是這些複雜的攻擊會導致具有破壞性的影響，我們預測在 2013 年在這方面會有更多的威脅出現。



(圖 3)一些針對核心顯著的攻擊在這幾年來有增加的趨勢

Windows 8 是下一個最大的攻擊目標

在很多情況之下，犯罪者攻擊的目標是使用者而不是作業系統，透過網路釣魚或是其他技術來欺騙使用者洩漏資訊或是安裝惡意軟體，所以並不能夠單純的透過 Windows 來保護使用者的系統，而是必須對這些保持警覺以防被騙。

與早期的 Windows 版本比較起來，Windows 8 雖然在安全性上強化了，藉此防止惡意軟體和漏洞滲透，但這也只能夠維持一段時間。就現在來看地下市場裡面的惡意軟體套件比起三年前來說，是更具有競爭力，針對 Windows 8 的惡意軟體提供的速度或許會比針對 Windows 7 的還來的快，根據某家研究公司表示新的系統仍會受到基於 MBR-rootkit 的攻擊。在 Windows 8 發佈之日，該公司便宣布將出售一個可用的零時差漏洞，以便用來強化 Windows 8 和 Internet Explorer 10 的安全性。

大規模攻擊

以往破壞電腦的惡意軟體已經越來越少見了，攻擊者開始傾向於利益導向或是竊取受害者電腦資訊，但是最近我們看到一些攻擊主要是具有針對性的，其他則像是蠕蟲等，此攻擊的唯一目標主要是盡可能造成大規模的傷害，我們相信這種惡意行為在 2013 年會有增長的趨勢。

在此最令人擔憂的事實是許多企業很容易受到這種大規模的攻擊，分散阻斷式攻擊(DDoS)雖然在技術上的障礙很低，但是如果攻擊者在大量的電腦上安裝具有破壞性惡意軟體的話，那麼其結果是具有毀滅性的。

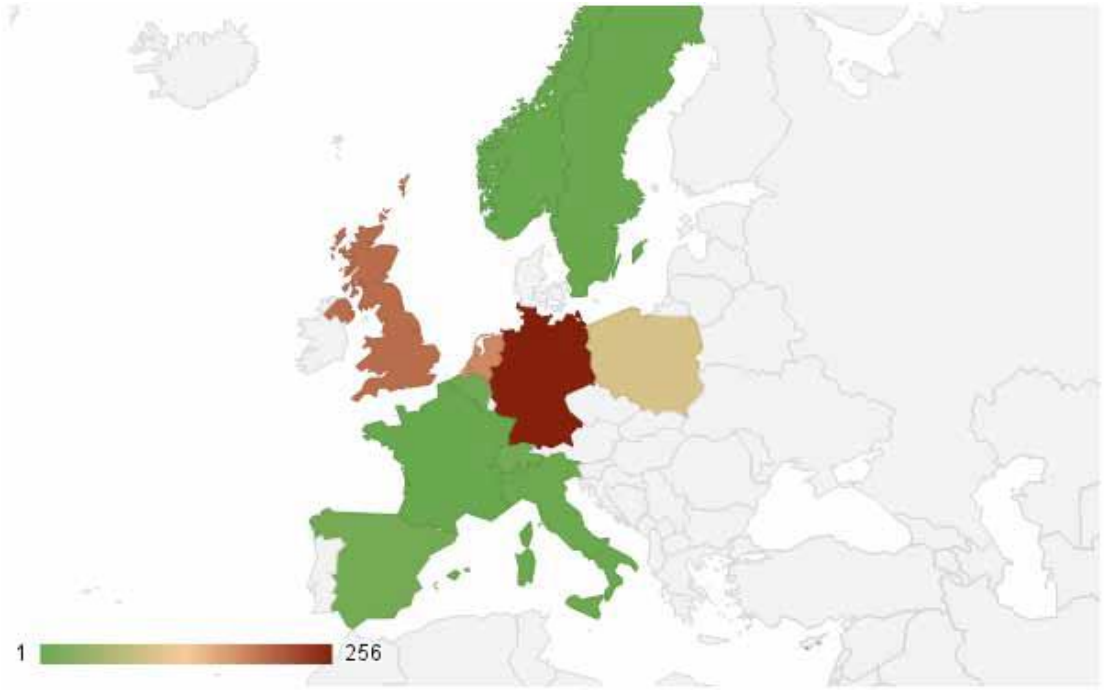
那我們該對這樣的事件做準備以減輕或防止傷害？從最壞的打算來看的話，除了業務網路、SCADA 系統等完全分隔控管之外，當企業遭受到攻擊的時候，當務之急是要恢復業務的營運，日後對內部所有機器做檢查的動作，以便確保惡意軟體是否完全清除。

採取這些措施同樣也能夠用來偵測和防止持續性威脅的攻擊，透過遠端應用程式的控制能夠讓駭客掌控伺服器與系統，因此可以透過系統監控來進行管理，為了確保資訊遺失降到最低，網路備份與恢復是必然的，同時備份與阻止攻擊者從網路芳鄰中獲得存取資料。

Citadel 木馬 Zeros In

Citadel 逐漸成為犯罪者對於木馬的選擇之一，因為 Citadel 具有 Zeus 豐富的功能與專門的支援，最新發佈的 Citadel 版本 Citadel Rain 能夠動態獲得配置檔案，讓攻擊者能夠寄送具有針對性的 payload 給所選擇的單一目標或是目標群，這使得攻擊者能夠根據自己的標準來進行目標式攻擊，相對之下，這方面的偵測也更加

困難，大都等到有受害者出現時才發現，因此對於 2013 年來說，將會有越來越多的犯罪者採用這些變種來進行針對式攻擊以尋求最大利益。



Citadel 木馬主要是在東歐比較盛行，特別是德國。我們預測 2013 年來自此惡意軟體的攻擊將會增加。

HTML5

HTML5 是網路瀏覽器標準語言的下一個版本，提供語言上的改進，功能包含不在需要套件、新的網頁框架選項、強大的 API、支援本地端儲存設備的存取等。現今 74%北美洲的使用者、72%的亞洲使用者和 83%的歐洲使用者所使用的瀏覽器有支援 HTML5，基於使用 HTML5 的使用者越來越多的情況之下，跨瀏覽器與設備之間的兼容性也正在持續改進中。

瀏覽器是資訊安全威脅中重要的傳播媒介之一，當然 HTML5 也不例外，隨著 HTML5 的普遍，攻擊者透過媒體與 API 對其進行攻擊，所提供的附加功能，允許設備直接存取網站硬體的 JavaScript API 也成為攻擊者的攻擊方式之一。

其中一個例子是 WebGL，主要提供 3D 渲染的功能，以往的 WebGL 主要是透過瀏覽器的套件讓 HTML 的內容能夠解釋與呈現出來，但是 HTML5 主要提供了能夠讓不受信任的資料在網路和作業系統進行直接溝通，因此這也成為攻擊者的攻擊媒介。

我們確信 2013 年攻擊者將會針對 HTML5 的安全去找出其漏洞，目前的問題只

在於到他們找出來以前時間還有多久而已。

殭屍網路與垃圾郵件

殭屍網路與其控制者回報狀態

對於殭屍網路控制者而言，最大的損失就是失去底下殭屍的控制，在過去幾年來，殭屍網路透過垃圾郵件和惡意軟體來進行散播感染的行為，並且根據其活動與成本來進行攻擊(像是 DDoS 等)，當最大的殭屍網路被阻絕之後，另一個最大的殭屍網路便會立即重現，同時殭屍網路也已經發展到「分支」的出現，導致殭屍網路幾乎無法完全移除，在某些情況之下，這些殭屍網路會被研究人員所操作以便用來觀察，但是當殭屍網路控制者發現與底下失去聯繫時，有時候可能會出現負面效果而導致其他層面的損害。

我們預計在 2013 年，殭屍網路將會變得更具有規模性，並繼續從事更高價值的商業攻擊活動。

“Snowshoe”發信將會持續增加

公司每天幾乎都會收到各式各樣的垃圾郵件，而這些郵件大多都是透過主機託管服務的主機所發送，有時後阻擋的手法就是將其永久列入黑名單中，但是雪靴發信，可以快速透過改變不同的 IP 或網域進行垃圾信的發送，持續對收件者的信箱做垃圾郵件的轟炸。“Snowshoe”發信主要是在過去兩年內爆發的，對於目前來說，垃圾郵件是世界面臨的最大問題之一，雖然研究人員試圖揭露這種威脅活動，但是在這以經濟利益為主的環境中，我們看到這種活動只會繼續以極快的速度增加。

來自受感染手機的垃圾簡訊

行動裝置提供商也正努力防止垃圾簡訊，消費者如果接收到垃圾簡訊，可以透過將此簡訊轉發至 7726 以便供應商阻擋此簡訊。另外受害者所會面臨的問題就是受感染的手機會寄發垃圾簡訊，而行動裝置提供商對此就是進行關閉帳戶的動作。我們預期在 2013 年將會有釣魚的垃圾簡訊出現。

犯罪軟體

入侵服務

網路犯罪份子會開始出現在論壇上與其他犯罪份子討論並且進行惡意軟體交易，同時也提供軟體服務，不過這有時候會遇到臥底或是虧損的情況，所以基於這些理由，論壇在註冊方面需要有額外的註冊費與擔保人機制。

這種趨勢會逐漸增加，對於那些購買卻不願透漏姓名的買家，也由於銷售網站模仿合法網站的方式持續增長中，因此有興趣購買的買家能夠透過滑鼠選擇惡意軟體套件，並選擇支付的方式，其中包含匿名付費等等，藉此避免交易行為不需要買家與賣家接觸或是有談判的行為產生。

(圖 4)買方找尋犯罪軟體的購物車

更多安全且匿名的優惠能夠在網路上尋找到，並且更加多元化，網路犯罪者除了高層次的審計服務之外，還提供客製化的項目開發服務，因此就目前的情況來看，如何分辨出合法與非法的網站與目標是很困難的。

(圖 5)入侵服務廣告

駭客行動主義

Anonymous 勢力衰退

由於太多不協調與不明確的行動以及虛張聲勢，駭客組織在 2013 年預計其發展將逐漸緩慢，Anonymous 目前技術發展已停滯很久，使用的攻擊手法已被大家所知道，因此攻擊成功的機率下降，所以我們預計 Anonymous 在數量與攻擊複雜性這兩方面均呈現下降的趨勢。

雖然到目前為止，由愛國主義者自動發起所組成的網路軍隊影響尚未深遠，但是他們行動的複雜度和攻擊性都將會得到提升，預計在 2013 年，全球將會有越來越多類似的網路軍隊前往社交網路的攻擊前線。

國家和軍隊成為網路威脅的參與者與受害者機會將越來越頻繁

世界軍事單位是社交網路的最前端，除了彼此之間的通訊越頻繁，軍事行動更會

使用網路來寄發電子郵件，但這些有可能造成資訊洩漏或是遭到滲透的可能性。

因此，專家們不再像傳統的方式預測攻擊所造成的物理傷害，而是藉由網路所導致的傷害與損失，其中有些攻擊伴隨著零時差漏洞與電子郵件則是會被認定為是進階持續性滲透攻擊。

攻擊者雖然不會對非戰鬥目標進行網路攻擊，但是一些網路犯罪份子卻已在網路招兵買馬、宣傳與招募資金，藉此準備佈署其攻擊，同時與國家相關的威脅也持續增多，當然疑似由國家所支援的攻擊也持續增加，不過我們並沒有適當的證據來證明，所以我們預測這樣的攻擊在 2013 年來說並不是一個空想。