2013 第三季的惡意郵件報告

原文出處： securelist http://www.securelist.com/en/analysis/204792311/Spam_in_Q3_2013

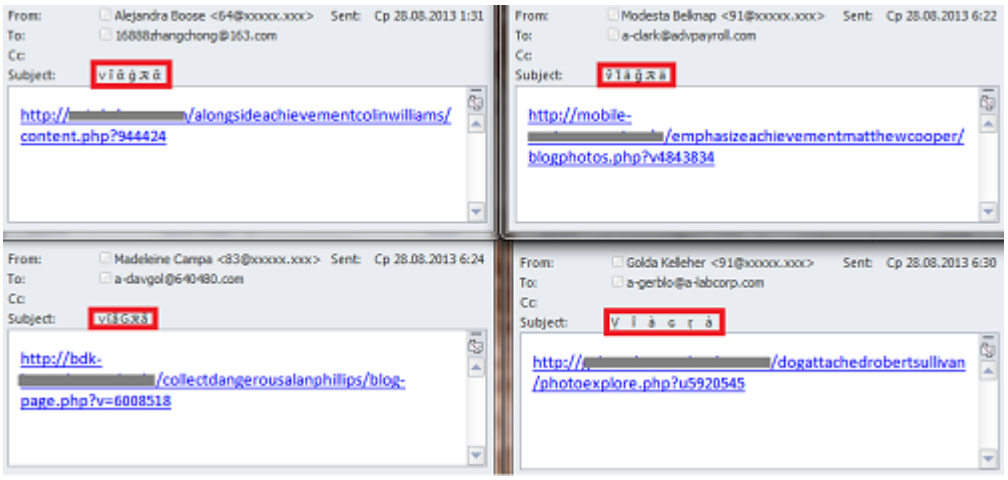
季統計表

垃圾郵件佔所有郵件的百分比與 2013 第二季相比下降了 2.4%，來到了 68.3%。釣魚郵件的百分比則增長了三倍，佔 0.0071%。惡意附件檢測到佔所有郵件的 3.9%，比 2013 年第二季少了 1.6 個百分點。

回到基礎面

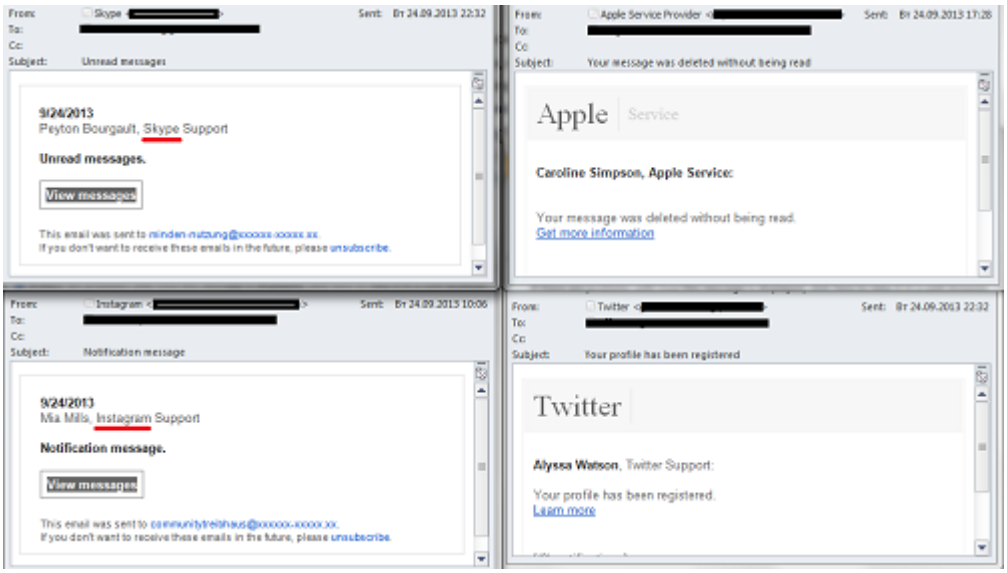
2013 的第三季，垃圾郵件發送者熱衷於典型藥物推廣的郵件來提升郵件效力特別是創意結合社交工程技術與技巧來繞過垃圾郵件過濾器。

在一個群體發送郵件當中，他們使用下面的方法：電子郵件的主題會用一個符號字串設計成類似 ‘Viagra’的字，而文字會被限制到一個醫藥網站的連結。



這種極簡方法可以幫助繞過內容過濾，沒有任何字會被發現，因為單詞”‘Viagra’不能被過濾器讀取辨別出來。即使他對人類來說是很容易可以辨別的。由於每封郵件都發現了不同的碼來代表 Viagra，所以簡單地添加新的關鍵字數據庫是不夠的。由於 UTF-8 包括所有語言的符號 - 包括非常罕見的符號。大多數語言都有自己獨特的字母，修飾字和符號，即使它們是基於熟悉的拉丁字母。因此，有超過 100 個符號，可以被讀作字母“a”。這並不奇怪，有成千上萬個潛在的不同組合，可以拼出'Viagra'。

另一個群發郵件發送的行為是發送一些熱門的電子郵件或是社交網路資源去鼓勵收件者去註冊，讀取新的訊息或是回應一個發送失敗訊息。然而，使用者如果點擊鏈接會被發送到已被攻破的網站並且重新導向到線上藥物商店，藉此來增加其效能。



郵件群體發送的作者模仿了許多公司的通知，包括 Apple, Yahoo, Google, Amazon, eBay, Twitter, Instagram, Skype,等，垃圾郵件發送者沒有投入大量的精力在這些消息的通知：代表發送假冒電子郵件的不同公司使用相同的模板設計，只有將公司名稱變更而已。

有趣的是，這種方式（假通知，一個妥協的網站和重定向到最終網站的連結）經常被垃圾郵件發送者用來散佈惡意程式碼。這種類型的垃圾郵件是透過合作夥伴的計劃，垃圾郵件發送者會從每一個用戶的點擊連結中獲取利益。這和廣告郵件的形式是相同的，只是垃圾郵件發送者會透過這些散佈的連結，從每一個藥丸的銷售中獲取回扣佣金。這意味著，攻擊者使用同樣的戰術但不同的合作夥伴計劃。在第三季，我們記錄的案例有兩種不同的合作夥伴計劃使用相同的群發郵件方式。電子郵件中的連結會依據不同的區域或是目前的時間而導向至不同的資源網站。舉例來說，用戶所在國家的藥物僅限處方才能獲取，那這些用戶就會被導向到 Viagra 網站。而所有其他的收件人則會被重新導向到一個欺詐或惡意的資源網站。

然而，另一種垃圾郵件的群體發送郵件會利用社交工程技術（假的通知從一個受歡迎的資源網站）和連結混淆。

電子郵件模仿 Google 的消息通知中心服務。郵件正文中包含了連到 Google 的連結。事實上，垃圾郵件發送者使用了 Google 翻譯的服務，以掩蓋自己的網站，他們做了一個翻譯的網站地址的請求。騙子並不需要任何真正的翻譯，網站本來就是英文的，只是再被翻譯成英文一次。垃圾郵件發送者還有另外一招，連結(每封電子郵件都會不一樣)當中的一些字符會被替換成相對應的十六進制的 ASCII。瀏覽器會很容易識別到這個混淆的連結，並且打開這個相對應的網站，但對垃圾郵件過濾器來說每一個連結都顯得很獨特。

新聞以及惡意軟體

2013 發生了許多一般大眾感興趣的事件。像是英國皇家新成員的誕生、FBI 追捕 Edward Snowden 以及西班牙的火車事故。而這些新聞都被詐騙者用來傳播惡意軟體。

Reports: Snowden able to leave Moscow airport

By CNN Staff July 24, 2013 – Updated 1315 GMT (2115 HKT)

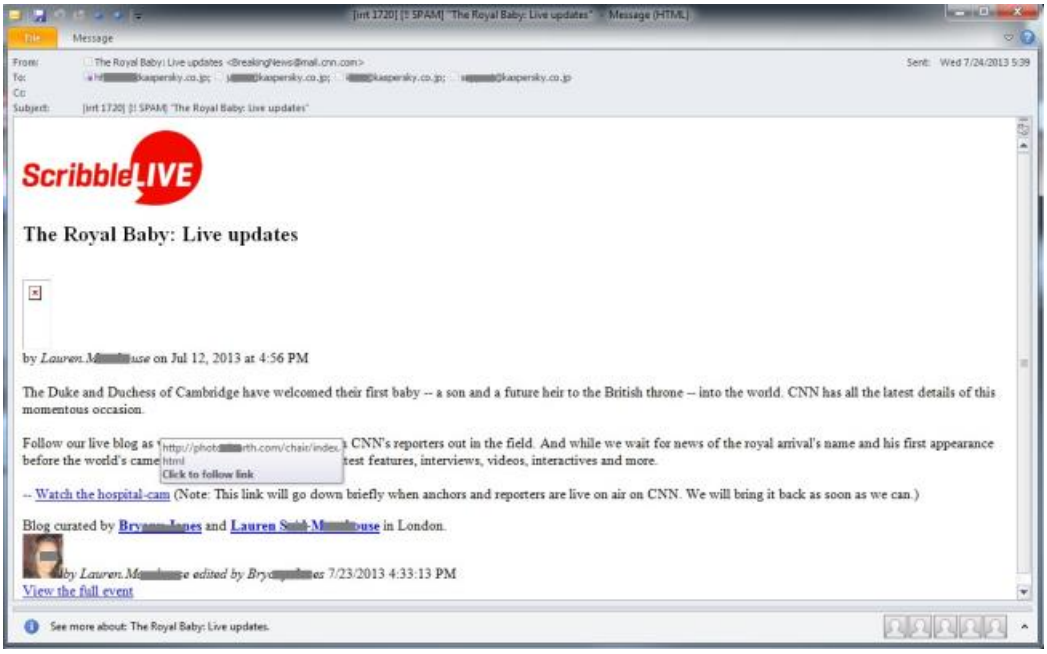
A picture of Snowden is displayed during a demonstration on July 4 in Berlin.

- Reports: Snowden could wait elsewhere in Russia while asylum request considered
- Snowden, whose U.S. passport was revoked, has been holed up at Moscow airport since June 23
- Snowden charged with espionage in U.S. after admitting to leaking info

(CNN) -- Russia has given U.S. intelligence leaker Edward Snowden a document that would allow him to leave a Moscow airport and wait somewhere else in the country while his temporary-asylum request is considered, Russian news media reported Wednesday.

Interactive: Snowden's options

(Ctrl)



ScribbleLIVE

The Royal Baby: Live updates

by *Lauren.M[redacted]use* on Jul 12, 2013 at 4:56 PM

The Duke and Duchess of Cambridge have welcomed their first baby -- a son and a future heir to the British throne -- into the world. CNN has all the latest details of this momentous occasion.

Follow our live blog as [redacted] CNN's reporters out in the field. And while we wait for news of the royal arrival's name and his first appearance before the world's came[redacted]test features, interviews, videos, interactives and more.

-- Watch the hospital-cam (Note: This link will go down briefly when anchors and reporters are live on air on CNN. We will bring it back as soon as we can.)

Blog curated by [redacted] and [redacted] in London.

[redacted] edited by [redacted] 7/23/2013 4:33:13 PM

View the full event

See more about: The Royal Baby: Live updates.

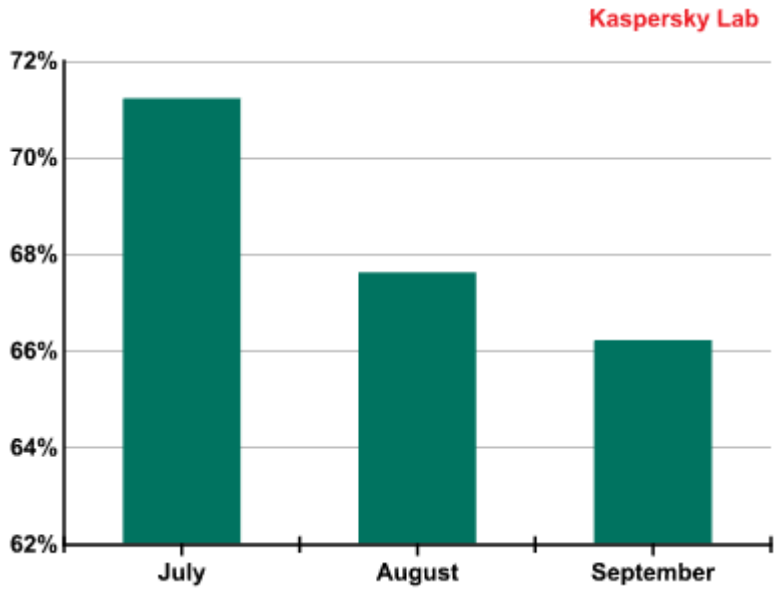
這些被卡巴斯基記錄下來的惡意郵件，在 2013 第 3 季以各種不同的形式出現，但大多是模仿大眾新聞郵件。然而，在所有電子郵件裡的連結會被導向到已被駭客攻破的網站，而這網站會重新導向用戶到一個頁面，並且伴隨了最流行的工具利用包套件-黑洞。一旦用戶訪問該網站，黑洞會開始尋找用戶軟體中的漏洞。如果找到漏洞，它會下載一些惡意程式，包括木馬間諜軟體，目的是要從受害者電腦中竊取個人的資料。

在十月的時候，黑洞的撰寫者，綽號大肚子(Paunch)，在俄羅斯被逮捕了。在未來這些工具包的利用情形仍是不明確的。不論是未來有人會接管黑洞套件工具包或是垃圾郵件發送者將遷移到其他的套件上。無論是哪種方式，未來新聞郵件的惡意案例可能比較少出現。

統計

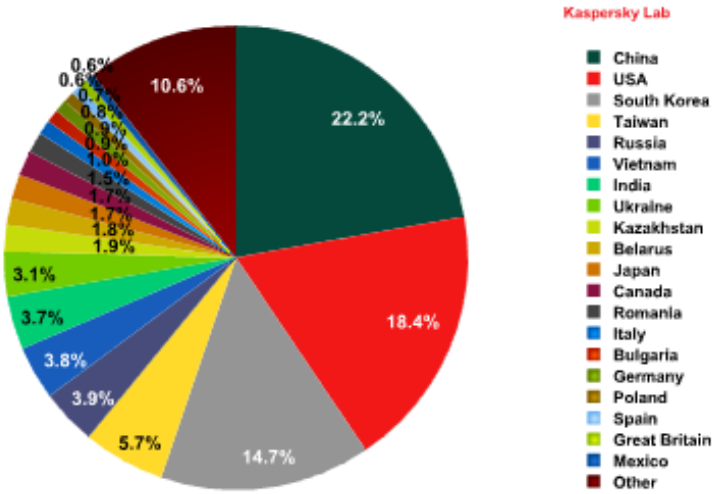
惡意郵件佔總電子郵件流量的百分比

總電子郵件流量中的垃圾郵件比例在今年的第三季，比第二季下降 2.4 個百分點來到了 68.3%。

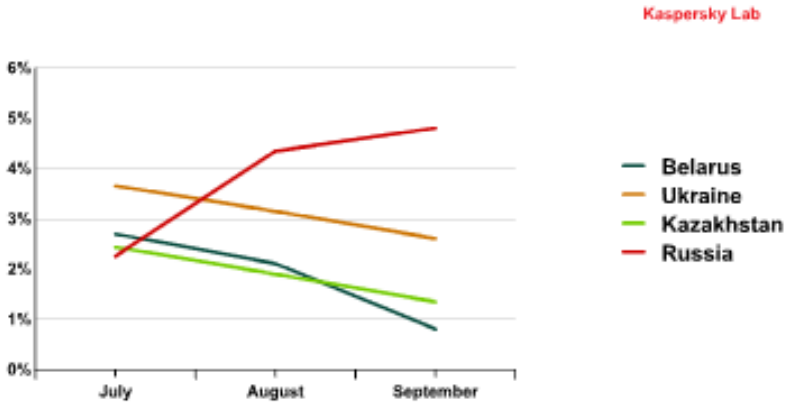


但是這種減少並不能看作一個開始的趨勢，在第三季的比例只有 0.3%，低於一到六月的平均指標。

垃圾郵件的來源國家



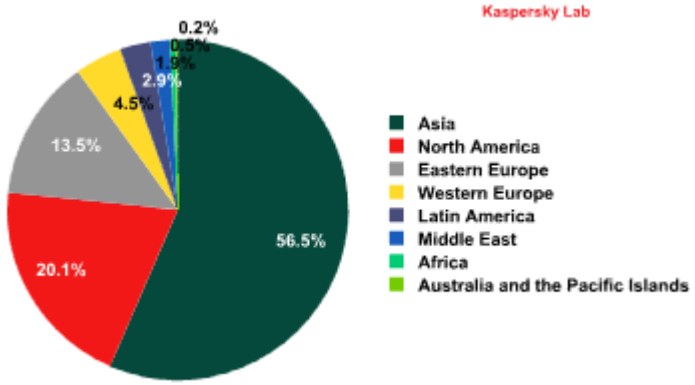
第三季前三名的垃圾郵件來源國家保持不變：中國（-0.9 個百分點），美國（1.2 個百分點）和韓國（2.1 個百分點）。這三個國家的總額佔全球垃圾郵件流量的 55%。截至上一季，台灣名列第四（+0.1 個百分點）。緊隨其後的是俄羅斯（1.3 個百分點），其增額增加了 1.5 倍以上。有趣的是，俄羅斯的垃圾郵件成長，正好與來自其他前蘇聯加盟共和國的垃圾郵件- 白俄羅斯（-0.9 個百分點），烏克蘭（-0.9 個百分點），哈薩克斯坦（-1.5 個百分點） 相對應。 而在 2013 年第二季這些下降國家產生的垃圾郵件則遠遠超過俄羅斯。



白俄羅斯，烏克蘭和哈薩克在 2013 年第三季的垃圾郵件百分比變化

然而，這並不一定意味著垃圾郵件發送者正在組織新的殭屍網絡：這種波動可能造成，例如，藉由傳播大規模郵件時交換一個存在的殭屍網路到另一個殭屍網路上。

垃圾郵件的區域來源



2013 第三季垃圾郵件的來源區域分配

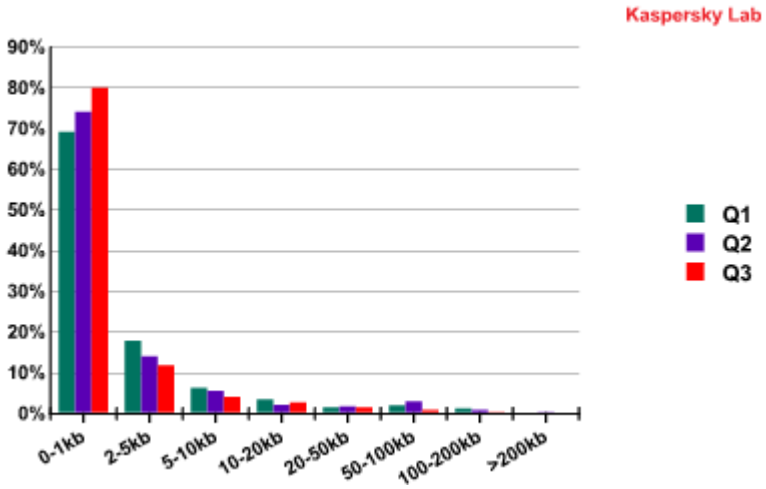
在第三季的垃圾郵件來源地區的最大來源國，並沒有任何大的變化，從 2013 年的前兩季開始。該地區的所佔比例也幾乎保持不變。

亞洲仍然是垃圾郵件來源區域的第一名（+0.2 個百分點）。其次是北美（+1.9 個百分點）和西歐（-0.2 個百分點）。

其他地區所在比例變化並不顯著。

值得注意的是，發送垃圾郵件與產生垃圾郵間之間並不總是有相關性。例如，很多非洲的垃圾郵件進入俄羅斯，對原產於韓國的郵件經常被送往歐洲，而來自西歐的垃圾郵件則均勻地分佈在世界各地。

垃圾郵件的大小



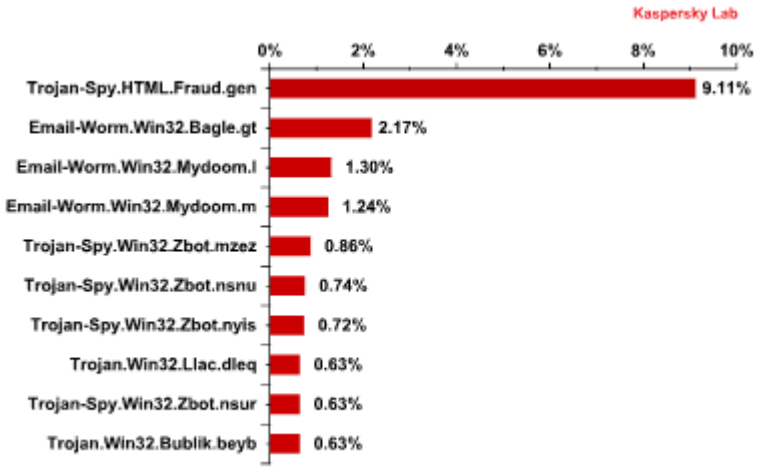
2013 第三季垃圾郵件的大小

從圖中可以看出，大小在 1KB 以下的小垃圾郵件的百分比每季都在成長。大多數這些電子郵件幾乎不包含任何文字。他們只包含一個連結，這通常會重新導向網站或短連結服務，這使得每封電子郵件有它的獨特性。這些郵件對郵件過濾器來

說增加了很多問題，由於其體積小，所以可以快速且發送數量巨大的垃圾郵件。

電子郵件的惡意附件

惡意附件第三季度的水平比第二季高出了 1.6 個百分點，來到所有郵件流量的 3.9%。



2013 第 3 季藉由電子郵件散佈的惡意程式前 10 名

在今年第三季的評比中。木馬 Spy.HTML.Fraud.gen 榮登最流行的惡意程式，透過電子郵件傳播，此惡意程式的設計看起來像一個 html 頁面，使用線上銀行註冊服務。釣魚者用它來竊取財務資訊。

截至上一季，電子郵件 Worm.Win32.Bagle.gt 排在第二。這種電子郵件蠕蟲，與其他不同的是可以發送給自己的副本、用戶地址簿中的聯繫人，並接收遠程端命令來安裝其他惡意軟體。

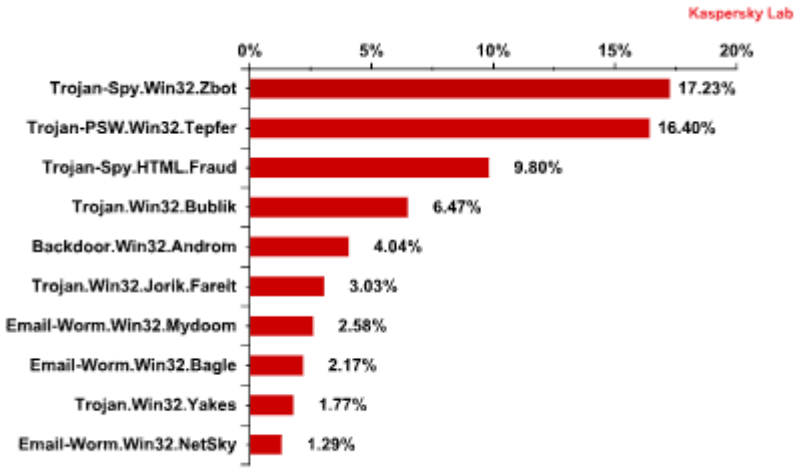
第三季的評比當中，兩個 Mydoom 的家族蠕蟲佔據第三和第四名，這些惡意程式目的在收集電子郵件地址，從用戶的地址簿。收集地址這種方法意味著您的電子郵件地址可能落入騙子手中，即使是不向大眾公開的。 Mydoom 家族是很老的家族，但它在電腦上仍繼續有效地的運作，不過它沒有持續做更新。電子郵件蠕蟲 Win32.Mydoom.m 可以發送隱藏的請求到搜索引擎。網站上顯示搜索結果中的第一頁，會與從欺詐者的服務器下載的地址進行比較。找到匹配項目時，它會打開搜索引擎頁面上的連結，從而提高特定網站在搜索結果上的排行。

ZeuS/ ZBOT 家族的代表佔據第五，第六，第七和第九位。這些惡意程式會從電腦竊取機密資料-通常是銀行信用卡的詳細資料 -。

Trojan.Win32.Llac.dleq 在第三季排在第 8 位。這個程式的主要任務是對用戶進行窺探監視：它收集有關安裝在電腦上軟體的訊息（主要是關於防病毒程序和防火牆部分），或 PC 處理器，作業系統，磁碟的相關資訊，它會攔截網絡攝像機的圖像和擊鍵（鍵盤記錄），並從各種應用程序中獲得豐富的機密資料。

Trojan.Win32.Bublik.beyb 來到第 10 名。此木馬的主要功能是偷偷下載並安裝惡意程式的新版本在受害者電腦上。它會以 Adobe PDF 文檔圖標的 EXE 文件形式出現。

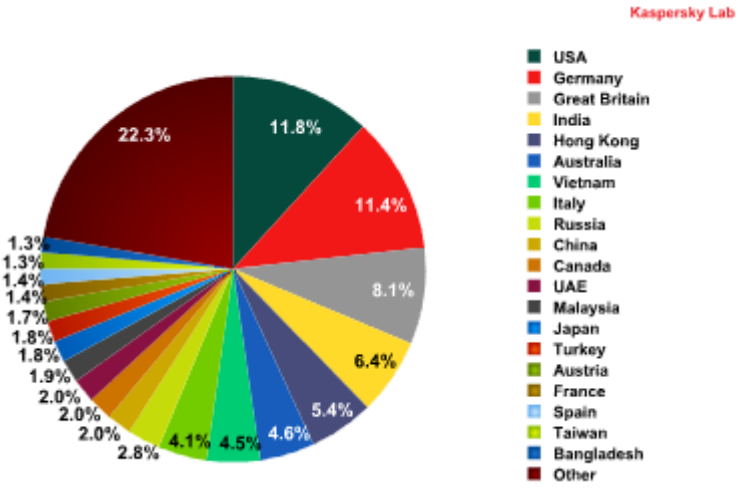
2013 年第三季透過電子郵件傳播的惡意程式的分佈如下：



2013 第三季經由電子郵件散布的惡意程式家族前十名

2013 年第三季的 ZeuS/ ZBOT 家族是第一名。其次是 Tepfer 家族，雖然沒有進入前 10 名。這種類型的木馬目的在竊取用戶的帳戶和密碼。詐欺木馬家族在第三位。Bublik 家族在第四位，第五名則是 Androm 家族，會在被害者電腦上下載並運行惡意文件。

最常被惡意電子郵件鎖定的目標國家名單從第二季以來已經發生了一些變化。



2013 第 3 季惡意電子郵件被偵測到的國家分佈

美國仍是第一名（-0.2 個百分點）。德國從第三上升到第二位，而俄羅斯則下降到第 9 位（-8.6 個百分點），接近平常一般的分佈。英國在第 3 名，其增長了 2.8 個百分點。

2013 年第三季裡，我們遇到了一個非常有趣的群體發送郵件-騙子模仿了大型防毒軟體公司技術支援服務的答覆。

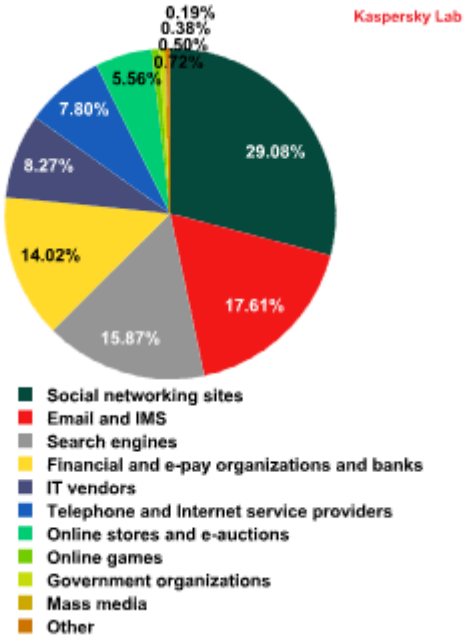
電子郵件會告知用戶該文件將被送往分析，結果會是惡意軟件。甚至命名為“技術支援工程師”的判決（在我們的例子中，mydoom.j），並會建議使用附加的簽名來消毒電腦，但如果用戶（當初可能沒有發送任何樣本）打開了附件，他們會

發現一個惡意程式，卡巴斯基防毒軟體會檢測到電子郵件蠕蟲 Win32.NetSky.q。

有趣的是，垃圾郵件發送者犯了一個錯誤：在“發件人”的欄位中，使用了賽門鐵克的技術支持服務的地址，同時在電子郵件的自動簽名命名另一個 – F-Secure 的防毒公司的官方地址。

網路釣魚

2013 年第三季的釣魚郵件比例比上一季增加了三倍，佔 0.0071%。



2013 第三季釣魚者鎖定的前 100 個目標組織總類分佈

第三季的通報顯示社交網站是最常被釣魚網站模仿的，郵件發送的服務以及搜尋引擎分別在第二和第三名的位置，事實上很難將這兩類分開，因為許多大公司將網路郵件跟搜尋引擎功能結合在一起。總體而言，這三類佔超過 60%的 100 大組織最常見有針對性的釣魚者攻擊。這一個數字顯示，被盜帳戶憑證的銷售是基於貨幣化的網絡釣魚。金融和電子支付組織以及銀行在釣魚者的目標清單中名列第四。這並不意味著網絡釣魚者對銀行不太感興趣。可能對個別攻擊的目標很少是在這麼大規模的機構當中，這也使它們進入了前 100 名。

結論

2013 年第三季垃圾郵件發送者積極利用舊的和新的招數來繞過郵件過濾以及利用社交工程技巧來說服使用者點擊必要的連結。例如，最常見的招數之一是使用高調熱門的新聞故事和設計成電子新聞郵件的形式來散布惡意軟體。

一些花招，比如代表一個知名的互聯網網站發送虛假的電子郵件，且常用於各種合作夥伴計劃，這招被認為是特別有效的。例如，模仿 Facebook 通知的電子郵件當中的連結，可以在不同的時間，在點擊連結後會重向導向到藥物廣告網站，或者導向到一個有漏洞的網站。

然而，遭逮捕的黑洞攻擊包的創造者已經表明，甚至在俄羅斯，其針對打擊網絡犯罪分子薄弱的立法下，網絡犯罪份子會繼續逍遙法外。

2013 第三季看到垃圾郵件來源的領先國家的變化不大。以區域的變化來看，甚至更少。殭屍網絡的位置似乎是相對穩定的，或者至少有一個平靜的殭屍網絡活動的搬遷的紀錄。

儘管電子郵件流量中垃圾郵件的所佔比例略有下降，惡意垃圾郵件的比例較上一季增長了 1.5 倍以上。大多數經由電子郵件傳播的惡意軟體會針對用戶的登錄密碼以及機密的財務資訊。

至於對釣魚者，對他們最有吸引力的目標是社交網站，電子郵件和其他的資源網站的使用者帳戶。