趨勢科技研究報告

網路犯罪地下經濟系列

2013 年中國地下市場

Lion Gu
前瞻威脅研究小組

內容

網路犯罪地下經濟系列

網際網路上存在著一些專門讓網路犯罪者聚集與買賣各種產品和服務的地方。他們可以向同行購買攻擊所需的工具，不需從頭自行開發，而且價格還頗競爭。這裡就像任何其他市場一樣，價格和功能也取決於市場供需法則。只是值得注意的是，近來市場上的價格有逐漸下滑的趨勢。

多年來，我們一直密切注意網路犯罪地下市場的重要發展，為的就是實現我們的願景：建立一個更安全的數位資訊交換世界。然而，多年來無時無刻都在監控網路犯罪活動的結果，也讓我們蒐集到更完整的市場情報，同時也掌握了這些市場的所有產品清單。

2012 年，我們發表了一份名為「俄羅斯地下犯罪網路初探」(Russian Underground 101) 的報告，文中介紹了俄羅斯網路犯罪地下市場的狀況。[1] 同年，我們也與「加州大學全球衝突與合作研究所」(University of California Institute on Global Conflict and Cooperation) 共同發表了「中國網路地下經濟調查」(Investigating China's Online Underground Economy) 一文，描繪了中國網路犯罪地下市場的狀況。[2] 去年，我們重新檢視了中國地下市場的情況並發表「網路犯罪不再只侷限於線上遊戲：重新檢視中國地下市場」(Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market) 一文。[3] 我們發現，每一個國家的地下市場都有其獨特性。為此，我們今年特別多收錄了一個新的市場，那就是：巴西。

網路犯罪的門檻正不斷降低，犯罪工具套件越來越普及、越來越便宜，某些甚至還能免費取得。價格不斷下滑、功能不斷增加，全球的網路地下論壇皆欣欣向榮，尤其是俄羅斯、中國和巴西，這些已成為各國境內駭客販售產品及服務給網路犯罪集團的熱門管道。此外，網路犯罪集團也透過所謂的深層全球網路 (Deep Web) 來販售一些全球網路 (World Wide Web) 的搜尋引擎所無法查到的產品和服務，為的就是要讓其網路店面不易遭到執法機關發現及破獲。

這一切的發展，意謂著一般大眾的運算環境受到攻擊的風險越來越高，因此，有必要徹底重新思考安全在日常資訊生活當中所應扮演的角色。

簡介

我們從 2011 年即開始持續監控中國地下市場的動態。截至 2013 年底為止，光在「QQ™ 群」上我們就發現了超過 140 萬則與地下市場相關的即時聊天訊息。

本文深入探討這數以百萬計的訊息，提出我們觀察到的趨勢以及 2013 年中國地下市場最新產品與服務的價格變化。

「QQ 群」遭到利用

網路犯罪集團利用熱門網站服務從事犯罪早已不是新聞，例如今年稍早，Dropbox 和 Evernote 服務就曾遭歹徒用於惡意程式的幕後操縱 (Command-and-Control，簡稱 C&C) 通訊。[4、5] 中國境內的網路犯罪亦不例外，他們也利用熱門的即時通訊軟體 QQ 作為通訊工具。

「QQ 群」是騰訊 (Tencent) 公司提供的一項即時通訊功能，可讓使用者輕鬆建立多個聊天群組，每一群組最多容納 2,000 名使用者。[6] 每一群組都有自己獨特的名稱、說明與使用者數量。QQ 群可讓人根據使用者數量或群組名稱及說明中的關鍵字來搜尋某個聊天群組。

圖 1：使用關鍵字「DDoS」搜尋 QQ 群的結果。

由於 QQ 群的功能完善、使用者數量龐大，現已成為地下市場歹徒聚集的主要場所。事實上，利用 QQ 來兜售犯罪軟體的網路犯罪集團甚至還建立了一些地下專有名詞來協助新手找到想要的東西。儘管這裡的產品/服務廣告刊登時間總是比專業地下論壇或網站的廣告來得短，不過，QQ 上的廣告卻比後者更新更頻繁。

圖 2：QQ 群的聊天畫面出現二則 DDoS 服務的廣告。

掌握了地下產品和服務所使用的熱門用語之後，我們就能找出需要監控的 QQ 群，進而追蹤使用者人數最多的群組。

2013 年中國地下市場統計數據

在 2012 年 3 月至 2013 年 12 月期間，我們從將近 500 個 QQ 群的 140 萬則訊息當中，找出了中國地下經濟的一些特性和發展趨勢。

2013 年過去的十個月當中，經由地下聊天群組所傳送的訊息數量較 2012 年同期成長了一倍，顯示地下市場的活動日趨頻繁。

圖 3：2012 和 2013 年地下聊天群組訊息數量比較。

另外，從 2013 年每小時的 QQ 群訊息數量顯示，從早上 8 點至晚上 10 點是使用者活動的時段，這或許意味著他們只是兼職從事地下市場交易。

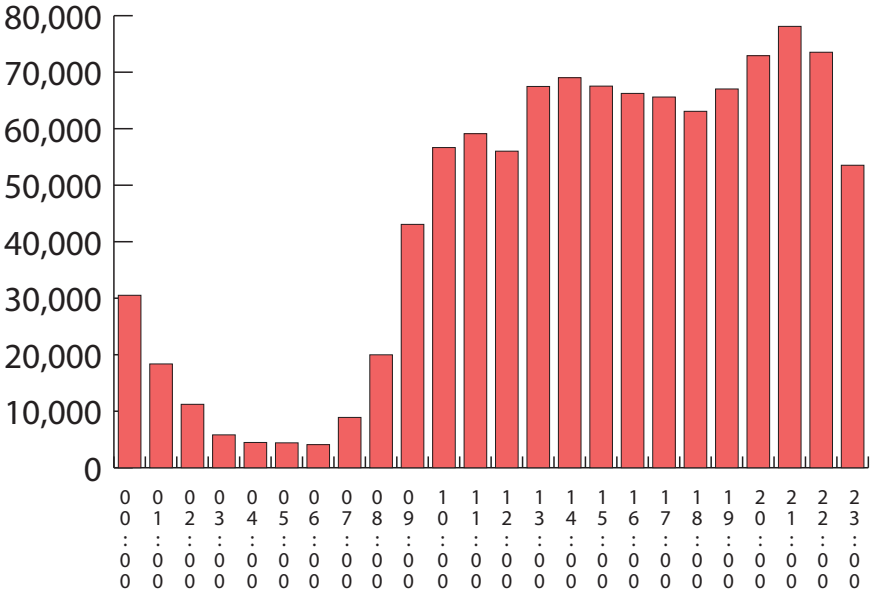

圖 4：2013 年地下聊天訊息每小時數量。

觀察同一群對象一整個星期的活動數據亦能證實這項理論，因為星期日的活動數量似乎較多。

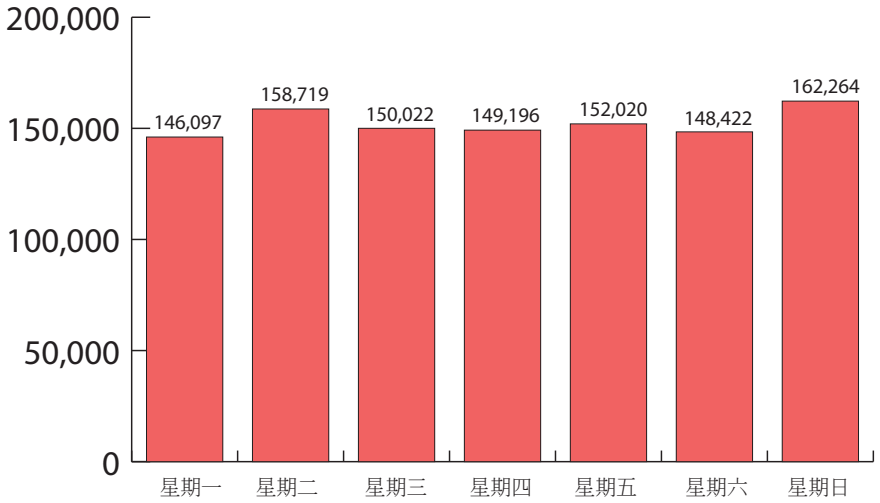

圖 5：2013 年地下聊天訊息每日數量。

我們設了一個新的指標：每一群組每日平均訊息數量 (簡稱 MGD) 來衡量 2012 年及 2013 年個別聊天群組的地下活動情況。該指標顯示每一群組的成員每日平均張貼的訊息數量。2012 年的平均值為 28.74，2013 年卻成長到 62.56，為前一年的二倍，這表示 2013 年地下聊天群組比 2012 年更加活躍。

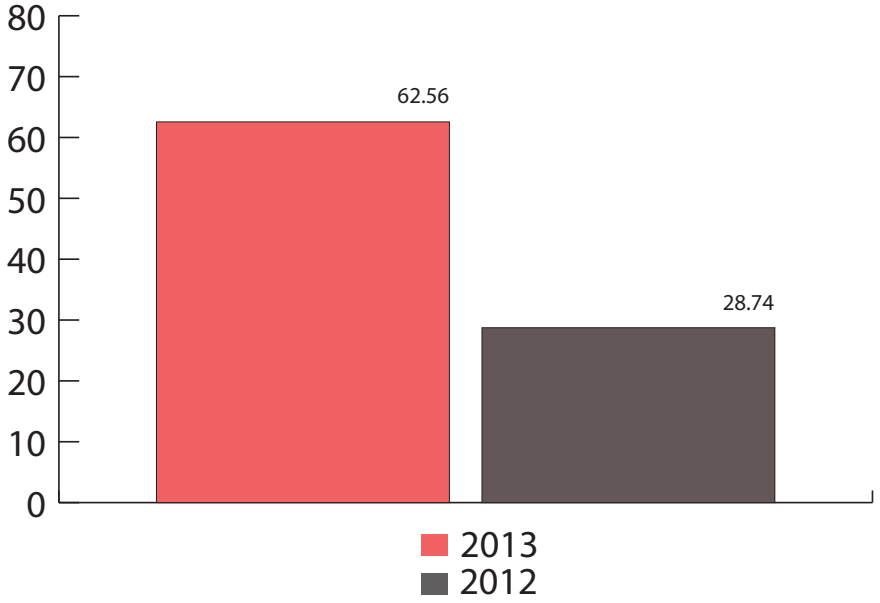

圖 6：2012 和 2013 年 MGD 比較。

如同所有線上聊天服務一樣，QQ 群會在記錄檔中顯示訊息張貼者的 ID 和匿稱，因此可以透過網際網路查到成員的更多相關資訊。例如，地下聊天成員數量從 2012 年至 2013 年明顯大幅增加。如同訊息數量一樣，聊天成員的數量在 2013 年的過去十個月較 2012 年同期成長了一倍。

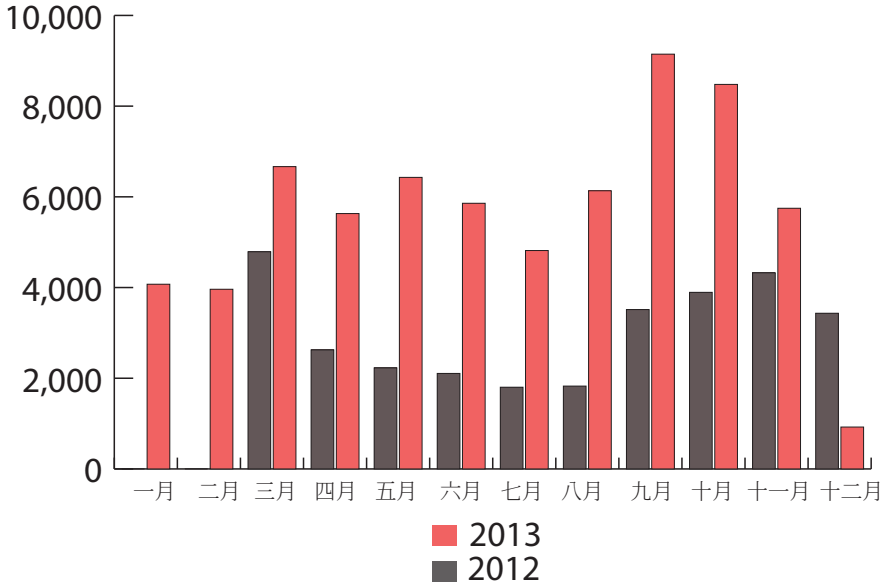

圖 7：2012 和 2013 年地下聊天成員數量。

我們又設計了另一個指標來衡量地下聊天群組活動：每一群組每日參與成員平均數量 (簡稱 PGD)。該指標顯示每一群組每日平均參與成員數量。我們發現 2012 年每一群組每日平均參與成員數量僅有 5.13，但 2013 卻成長到 11.26，表示有更多人對網路犯罪行業有興趣。

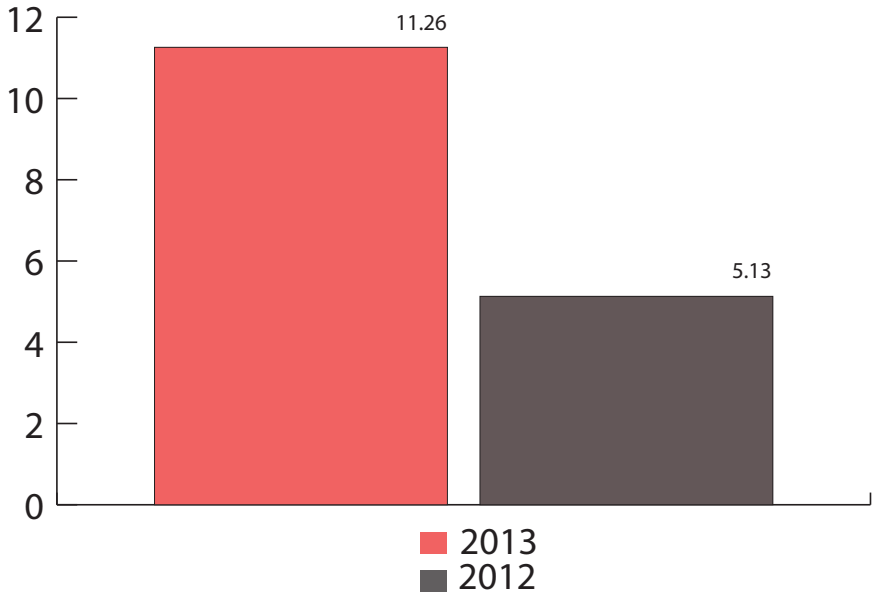

圖 8：2012 和 2013 年 PGD 比較。

此外，我們也探討了不同產品及服務在地下市場的熱門程度。這讓我們了解地下聊天群組的成員最感興趣的是哪種網路犯罪，地下市場專門用語確實有助於判斷每種產品或服務的熱門程度。中國地下市場最熱門的三項產品/服務分別為：已入侵的主機、分散式阻斷服務攻擊 (DDoS) 服務以及遠端存取工具/木馬程式 (RAT)。

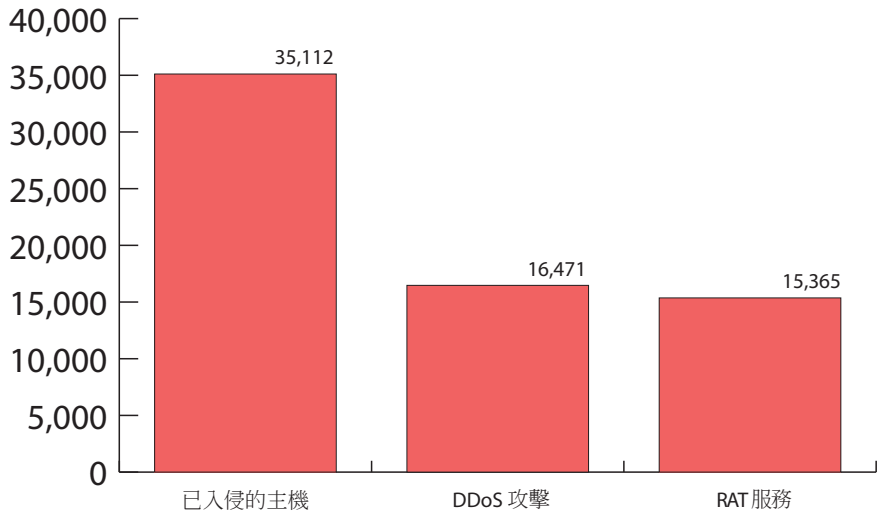

圖 9：2013 年地下市場最熱門的產品/服務。

已入侵的主機

所謂「已入侵的主機」是指那些網路犯罪集團可從幕後操縱而其系統擁有者卻不知情的主機。[7] 也就是說，犯罪集團可像本機系統管理員一樣使用該系統。一般來說，每台主機都有其特定的運算能力、儲存空間、網路頻寬、IP 位址以及敏感資料。這一切都可能遭網路犯罪集團用於從事犯罪，例如：

- **利用已入侵的主機來散布惡意程式或垃圾郵件。**網路犯罪集團可讓主機感染可傳染給其他相連系統與裝置的惡意程式，此外也能用它來發送垃圾郵件。

- **利用多台已入侵的系統來發動 DDoS 攻擊。**網路犯罪集團還能操縱大量已入侵的主機在同一時間連上某一個 IP 位址或 URL 網址，如此大量的網路流量將癱瘓該網站的伺服器而導致服務停擺。[9]

- **利用已入侵的主機來執行複雜的運算工作。**利用這類主機來開採比特幣 (Bitcoin) 即是一例。[10] 由於開採比特幣需要消耗大量的運算資源，這樣的作法讓網路犯罪集團不需提升自己的硬體就能輕鬆開採比特幣。

網路犯罪集團通常會利用下列方式來入侵主機系統：

- **順道下載攻擊。**網路犯罪者會上傳惡意程式 (通常是 RAT 遠端存取工具) 到一般合法的網站，然後利用誘人的社交工程誘餌讓使用者造訪這些網站。使用者一旦造訪這類網站，其電腦就會感染惡意程式。惡意程式一旦執行起來，網路犯罪集團就能從幕後操縱被感染的系統。[11]

- **遠端桌面連線。**許多連上網際網路的系統都沒有設定好系統安全性。因此，網路犯罪集團就能輕易透過「遠端桌面連線」取得系統的控制權。[12] 儘管這是一項可讓 IT 系統管理員從遠端存取系統以進行疑難排解和其他工作的正當功能，但系統若使用預設的連接埠 (3389) 而且又使用簡易的密碼，就很容易遭駭客入侵。事實上，這類被戲稱為「3389 主機」的系統在網際網路上比比皆是。

DDoS 攻擊服務

DDoS 攻擊可讓合法的線上服務中斷。[13] 在這類攻擊當中，網路犯罪集團會對目標伺服器送出超量的服務請求，導致服務因而癱瘓。 中國地下市場最常見的兩種 DDoS 攻擊服務為：

- **SYN 同步訊號洪水攻擊 (SYN flooding)**：同步訊號洪水攻擊的作法是發送大量的 TCP/SYN 封包到目標網站 (通常使用假的發送端位址)。[14] 由於每一封包都是一個建立連線的請求，因而導致伺服器回應大量的 TCP/SYN-ACK 封包並產生大量開啟到一半的網路連線來等待發送端進一步回應。然而，由於發送端位址其實是假的，因此伺服器永遠等不到回應，使得伺服器資源耗盡而癱瘓服務。

- **HTTP GET 網頁讀取請求洪水攻擊 (HTTP GET flooding)**：亦稱為「Challenge Collapsar (CC)」攻擊，專門攻擊網站伺服器。[15] HTTP GET 網頁讀取請求洪水攻擊是藉由發送大量的 HTTP GET 請求到目標 URL。回應網頁請求需消耗網站伺服器資源，如同查詢資料庫和從硬碟讀取檔案一樣。而回應大量的 HTTP GET 請求將消耗大量的系統資源，導致目標網站無法正常運作。

任何打算發動 DDoS 攻擊的網路犯罪集團都能在中國地下市場買到 DDoS 攻擊套件。DDoS 攻擊套件是一種讓遠端使用者能操控許多系統來發送大量網路封包到目標網站的工具套件。除了 SYN 和 HTTP GET 洪水攻擊之外，DDoS 套件還可用於 Internet Control Message Protocol (ICMP)、User Datagram Protocol (UDP)、ACK 以及其他類型的洪水攻擊。[16、17、18] 此外，地下市場也提供了一些已入侵的系統可用來發送封包到目標電腦，包括已入侵的主機及專用伺服器。

專用伺服器只提供租用服務，在租用期間，承租人可使用伺服器上的所有資源。有別於已入侵的主機，專用伺服器擁有更好的硬體及更快的網路連線速度。只要幾十台專用伺服器就足以發動一次攻擊行動。為了隱藏這些專用伺服器的位置，網路犯罪集團通常會在發送到目標的封包當中使用假 IP 位址。

圖 10：DDoS 攻擊套件主控台。

網路犯罪集團通常會直接對目標 IP 發動封包洪水攻擊。不過，有些也會對攻擊目標的網域名稱系統 (DNS) 伺服器發動封包洪水攻擊。只要 DNS 伺服器遭到癱瘓，任何該伺服器所管轄的網域名稱都將無法查詢，包括目標網域在內。因此，一旦 DNS 伺服器遭到攻擊而癱瘓，許多網站都將受到影響。攻擊 DNS 伺服器的工具在地下市場算是一項新產品。

RAT 遠端存取工具

RAT 可讓使用者從遠端存取並遙控系統。[19] 這些工具提供許多功能，涵蓋絕大多數的系統管理作業。他們原本的設計用意是為了讓系統管理員的工作更輕鬆，但現在卻因為能夠躲過偵測而被用於遙控目標系統。[20]

此外，RAT 也非常具有彈性。例如，網路犯罪集團可利用 RAT 來取得目標系統上的檔案清單，然後將某個檔案壓縮並傳送給自己。

2013 年中國地下市場販售之產品

前述三項產品/服務顯然是 2013 年中國地下市場最熱門的產品。除此之外，還有其他產品與服務可供任何有興趣者購買。

中國地下市場販售之產品		
產品	詳細內容	價格
殭屍網路 (Botnet)	Windows： • 100 台 Windows XP 殭屍電腦 • 100 台 Windows Server 2003/2008 殭屍電腦 DDoS 攻擊： • 100 台殭屍電腦 • 300 台殭屍電腦 • 800 台殭屍電腦 • 2,000 台殭屍電腦	8 美元 48 美元 95 美元 208 美元 386 美元 596 美元
漏洞攻擊套件	NB 漏洞攻擊套件	323 美元
假造貼文/回應/點閱/追隨者	「百度貼吧」論壇： • 100 則新貼文 • 100 則回應 10,000 個「優酷」視訊點閱 「新浪微博」部落格： • 100 名追隨者 • 1,000 名追隨者 • 3,000 名追隨者	16–48 美元 8–16 美元 0.65 美元 2 美元 13 美元 37 美元
假網站	QQ/淘寶/中國工商銀行 各種線上遊戲 線上遊戲交易網站	81 美元 16–32 美元 81–97 美元
掃描的偽造文件	中國/美國/加拿大護照	5 美元
序號/金鑰	Microsoft 產品： • Windows® 8 Pro • Windows Server 2012 R2 • Microsoft™ Office® 2013 Pro 其他產品： • Adobe® Photoshop® Creative Suite® 6 • AutoCAD® 2013	0.65–3 美元 0.81–2 美元 0.81–6 美元 0.81–3 美元 3–11 美元

中國地下市場販售之產品		
產品	詳細內容	價格
網路流量	每日 500 個 IP 位址 每日 1,000 個 IP 位址 每日 5,000 個 IP 位址 每日 10,000 個 IP 位址 每日 50,000 個 IP 位址 每日 100,000 個 IP 位址 每日 500,000 個 IP 位址	0.26 美元 0.42 美元 2 美元 5 美元 38 美元 95 美元 473 美元
木馬程式	QQ 帳號竊取程式 淘寶帳號竊取程式 雲騰銀行木馬工具套件： • 銅級 • 銀級 • 黃金級 • 白金級 • 鑽石級	32 美元 323 美元 1,273 美元 1,596 美元 2,080 美元 2,565 美元 3,856 美元

註：上表內的產品價格是以 2014 年 7 月 27 日人民幣對美元的匯率換算。
資料來源：51traffic.com、bw520.com、QQ 聊天訊息、taobao.com、tieba.baidu.com、www.07328.com、www.520banks.com、www.hangamei.com、www.wsddos.yulusa.com、youlong2013.com。

中國地下市場販售之服務		
服務	詳細內容	價格
破解	加密 .RAR、.ZIP、.DOC、.XLS 或 .EXE 檔案 軟體： • Dongle 保護 • 註冊碼 • 使用者數量限制保護	45 美元 807–12,919 美元 161 美元 242 美元
專用/防攻擊 (Bulletproof) 伺服器代管	一個月 (含 DDoS 攻擊防護)	81–775 美元
DDoS 攻擊	1GB 封包： • SYN (每日) • HTTP GET (每日) 每日 10GB SYN 封包 DNS 伺服器攻擊 DDoS 攻擊套件租用： • 一個月 • 六個月 • 一年 • 終生	 16 美元 73 美元 161 美元 323 美元 81 美元 161 美元 258–323 美元 452–484 美元

中國地下市場販售之服務		
服務	詳細內容	價格
偽造文件重製		19 美元
駭客破解	論壇帳號： • 一般使用者 • 論壇分區管理員 • 論壇管理員 • VIP QQ 帳號： • 密碼 • 六個月聊天記錄 • 一年聊天記錄 電子郵件帳號： • 個人 • 企業 新浪/微博/人人帳號	81 美元 161 美元 323 美元 官網服務費的 30% 48 美元 81 美元 129 美元 48 美元 81 美元 48 美元
確認惡意程式是否能躲過資訊安全軟體檢查	各種軟體	13–19 美元
程式設計	RAT 工具套件 木馬程式	161 美元 323–8,075 美元
代理 (Proxy) 伺服器代管	HTTP SOCKS 代理伺服器： • 每月單一固定 IP 位址 • 每月 800 個 IP 位址 • 每月 9,000 個 IP 位址 • 每月 32,000 個 IP 位址	4 美元 0.16 美元 2 美元 16 美元
RAT 工具套件租用	TYT/MBZ RAT 每年 RD RAT： • 一個月 • 一年	97 美元 129 美元 258 美元
散發垃圾郵件	1,000 封垃圾郵件 10,000 封垃圾郵件 20,000 封垃圾郵件 50,000 封垃圾郵件 100,000 封垃圾郵件	13 美元 97 美元 161 美元 323 美元 484 美元
木馬程式攻擊	每日一個線上遊戲	29 美元

中國地下市場販售之服務		
服務	詳細內容	價格
VPN 伺服器代管	一個月 三個月 一年	3 美元 8–10 美元 19–32 美元

註：上表內的服務價格是以 2014 年 7 月 27 日人民幣對美元的匯率換算。
資料來源：173.252.233.132、17msge.com、blog.sina.com.cn、QQ 聊天訊息、task.zhubajie.com、wodexiangzi.com、www.2sxvpn.com、www.360email.cn、www.49207.com、www.512727.com、www.51cxjilu.com、www.71n.net、www.gyddos.com、www. jx39.com、www.killdog.net、www.nc2c.com、www.rmd5.com、www.sinogemsoft.com、 www.whenq.com。

中國行動裝置地下市場統計數據

針對行動電話使用者的攻擊不斷快速攀升，從 Android™ 惡意程式數量的快速成長即可證明。[21] 因此，我們也探討了 2013 年中國新興行動裝置地下市場的狀況。

針對本文，我們監控了 11 個行動裝置地下聊天群組 (包含在全部 500 個群組當中) 來看看行動裝置的每一群組每日平均訊息數量 (MGD)。我們發現，行動裝置的 MGD 為 61.3，也就是，地下行動裝置聊天群組每日大約張貼了 61 則訊息。此數字非常接近整體網路犯罪地下市場 2013 年的 MGD。對照 2012 年的 MGD，我們可發現 2013 年行動裝置地下市場的活動僅略微頻繁一點。

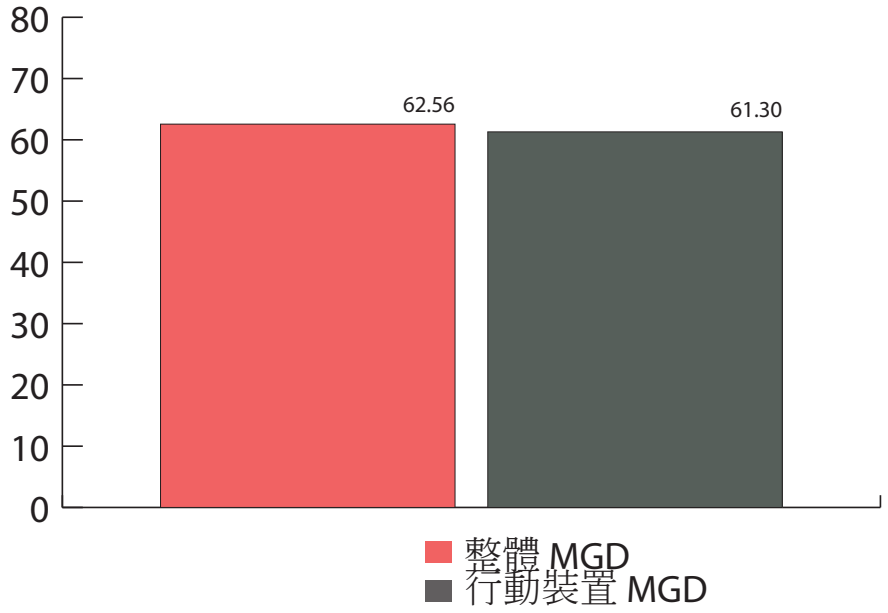

圖 11：2013 年整體 MGD 與行動裝置 MGD 比較。

此外，我們也探討了行動裝置每一群組每日平均參與成員數量 (PGD) 並且發現該數字從 2012 年的 11 人左右成長到 2013 年的 29 人左右。也就是說，2013 年每一個行動裝置地下聊天群組每天大約有 29 名成員參與，幾乎是 2012 年的 2.5 倍。此外，2013 年行動裝置 PGD 亦超過整體 PGD 的兩倍。

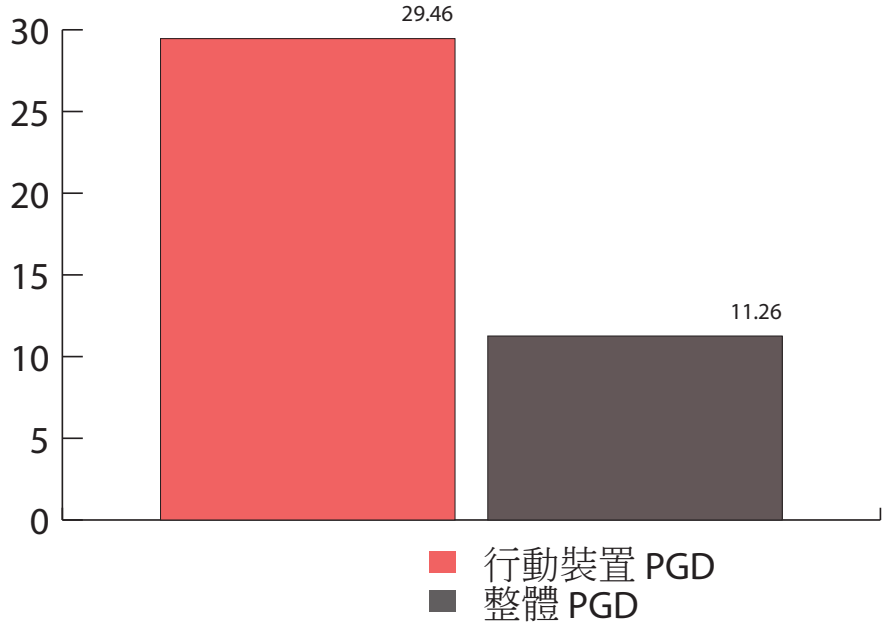

圖 12：2013 年整體與行動裝置 PGD 比較。

我們同時也探討了中國行動裝置地下市場最受歡迎的產品/服務，並且發現前三名分別是：垃圾簡訊散發服務、簡訊伺服器，以及高費率服務電話號碼。

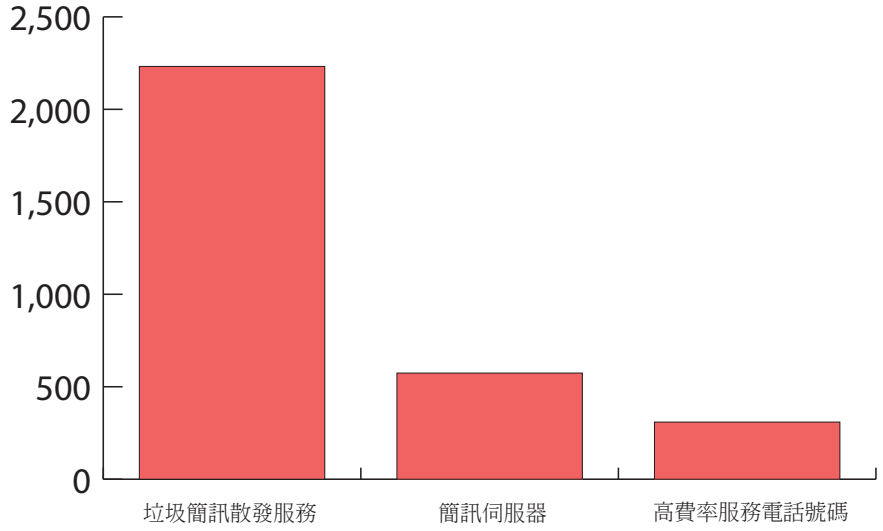

圖 13：2013 年行動地下市場最受歡迎的產品/服務。

如需更多有關中國行動裝置地下市場最受歡迎產品/服務及其他產品/服務的詳細內容和價格資訊，請參閱「中國行動裝置網路犯罪地下市場」(The Mobile Cybercriminal Underground Market in China) 一文。[22]

結論

本文根據我們 2012 年及 2013 年針對「QQ 群」的監控資料分析了中國地下市場的狀況。我們發現，2013 年中國地下市場的活動較 2012 年成長一倍，不論是參與的人數或產品/服務數量皆然。

已入侵的主機、DDoS 攻擊服務以及 RAT 遠端存取工具是中國地下市場上最受歡迎的產品/服務。此外，該國的行動裝置地下市場亦逐漸興起。垃圾簡訊散發服務、簡訊伺服器以及高費率服務電話號碼則是行動裝置地下市場最受歡迎的產品/服務。

總而言之，中國地下市場正緊跟著資訊安全領域的發展情勢。這些市場再也不只單純地兜售專門攻擊 PC 使用者的惡意程式，也攻擊快速成長的行動裝置。因此再次提醒我們，任何連上網際網路的電腦或裝置都應具備資訊安全防護，才能享受安全的數位生活。

參考資料

1. Max Goncharov。(2012 年)。*趨勢科技資訊安全情報*。「俄羅斯地下犯罪網路初探」(Russian Underground 101)。上次存取時間 2014 年 7 月 27 日：http://www.trendmicro.com/cloudcontent/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf。
2. Zhuge Jianwei、Gu Liang 和 Duan Haixin。(2012 年 7 月)。*IGCC*。「中國網路地下經濟調查」(Investigating China's Online Underground Economy)。上次存取時間 2014 年 7 月 27 日：http://igcc.ucsd.edu/publications/igcc-in-the-news/news_20120731.htm。
3. Lion Gu。(2013 年)。「網路犯罪不再只侷限於線上遊戲：重新檢視中國地下市場」(Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market)。 上次存取時間 2014 年 7 月 27 日：http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-beyond-online-gaming-cybercrime.pdf。
4. Maersk Menrige。(2014 年 6 月 25 日) 。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「內含定時炸彈的 PlugX RAT 程式利用 Dropbox 服務來進行幕後操縱設定」(PlugX RAT with "Time Bomb" Abuses Dropbox for Command-and-Control Settings)。上次存取時間 2014年 7 月 21 日：h ttp://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/。
5. Nikko Tamaña。(2014 年 3 月 27 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「後門程式使用 Evernote 作為幕後操縱伺服器」(Backdoor Uses Evernote as Command-and-Control Server)。上次存取時間 2014 年 7 月 21 日：http://blog.trendmicro.com/trendlabs-security-intelligence/backdoor-uses-evernote-as-command-and-control-server/。
6. 騰訊。(2014 年)。*QQ International*。「QQ International 官方部落格」。上次存取時間 2014 年 7 月 21 日：http://blog.imqq.com/。

7. Wikimedia Foundation Inc.。(2014 年 7 月 24 日)。*Wikipedia*。「殭屍網路」(Botnet)。上次存取時間 2014 年 7 月 25 日：http://en.wikipedia.org/wiki/Botnet。

8. Maria Manly。(2014 年 4 月 24 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「AOL 郵件服務遭駭，受害電子郵件帳號被用於散發垃圾郵件」(AOL Mail Service Hacked, Compromised Emails Used to Send Spam)。上次存取時間 2014 年 7 月 25 日：http://blog.trendmicro.com/trendlabs-security-intelligence/aol-mail-service-hacked-compromised-emails-used-to-send-spam/。

9. Chris Huang。(2013 年 4 月 16 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「殭屍網路涉及匿名分散式阻斷服務 (DDoS) 攻擊」(Botnets Involved in Anonymous DDoS Attacks)。上次存取時間 2014 年 7 月 25 日：http://blog.trendmicro.com/trendlabs-security-intelligence/botnets-involved-in-anonymous-ddos-attacks/。

10. Karl Dominguez。(2011 年 9 月 4 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「開採比特幣的殭屍網路出現分散式阻斷服務 (DDoS) 攻擊能力」(Bitcoin Mining Botnet Found with DDoS Capabilities)。上次存取時間 2014 年 7 月 25 日：http://blog.trendmicro.com/trendlabs-security-intelligence/bitcoin-mining-botnet-found-with-ddos-capabilities/。

11. Jonathan Leopando。(2010 年 10 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「諾貝爾和平獎網站遭人植入 Firefox 零時差攻擊」(Firefox Zero-Day Found in Compromised Nobel Peace Prize Website)。上次存取時間 2014 年 7 月 25 日：http://blog.trendmicro.com/trendlabs-security-intelligence/firefox-zero-day-found-in-compromised-nobel-peace-prize-website/。

12. Microsoft。(2014 年)。*Windows*。「遠端桌面連線」(Remote Desktop Connection)。上次存取時間 2014 年 7 月 25 日：http://windows.microsoft.com/en-us/windows7/products/features/remote-desktop-connection。

13. 趨勢科技。(2014 年)。*威脅百科網站 (Threat Encyclopedia)*。「分散式阻斷服務 (DDoS) 攻擊」(Distributed Denial of Service)。上次存取時間 2014 年 7 月 25 日：http://about-threats.trendmicro.com/us/definition/distributed-denial-of-service-ddos。

14. Wikimedia Foundation Inc.。(2013 年 12 月 28 日)。*Wikipedia*。「SYN 洪水」(SYN Flood)。上次存取時間 2014 年 7 月 25 日：http://en.wikipedia.org/wiki/SYN_flood。

15. Neustar Inc.。(2014 年)。*DDoSAttacks.biz*。「HTTP GET 洪水分散式阻斷服務攻擊，亦稱為 HTTP 物件請求洪水」(HTTP GET Flood DDoS Attack, aka HTTP Object Request Flood)。上次存取時間 2014 年 7 月 25 日：http://www.ddosattacks.biz/attacks/http-post-flood-ddos-attack-definition-mitigation/。

16. Wikimedia Foundation Inc.。(2014 年 7 月 26 日)。*Wikipedia*。「網際網路控制訊息通訊協定」(Internet Control Message Protocol)。上次存取時間 2014 年 7 月 27 日：http://en.wikipedia.org/wiki/Internet_Control_Message_ Protocol。

17. Wikimedia Foundation Inc.。(2014 年 7 月 4 日)。*Wikipedia*。「使用者資料封包通訊協定」(User Datagram Protocol)。上次存取時間 2014 年 7 月 27 日：http://en.wikipedia.org/wiki/User_Datagram_Protocol。

18. Staminus Communications。(2013 年 9 月 24 日)。「DDoS 攻擊種類：ACK 洪水」(Types of DDoS: ACK Flood)。上次存取時間 2014 年 7 月 27 日：https://wiki.staminus.net/index.php/Types_of_DDoS:ACK_Flood。

19. 趨勢科技。(2014 年)。*威脅百科網站 (Threat Encyclopedia)*。「遠端存取程式/工具」(Remote Access Programs/Tools)。上次存取時間 2014 年 7 月 27 日：http://about-threats.trendmicro.com/us/definition/remote-access-programs-tools。

20. Rhena Inocencio。(2014 年 5 月 26 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「Blackshades 遠端存取工具：入門級網路犯罪」(The Blackshades RAT—Entry-Level Cybercrime)。上次存取時間 2014 年 7 月 27 日：http://blog.trendmicro.com/trendlabs-security-intelligence/the-blackshades-rat-entry-level-cybercrime/。

21. 趨勢科技。(2014 年)。*威脅百科網站 (Threat Encyclopedia)*。「TrendLabs 2014 年第二季資訊安全總評：扭轉網路攻擊局勢」(TrendLabs 2Q 2014 Security Roundup: Turning the Tables on Cyber Attacks)。上次存取時間 2014 年 8 月 12 日：http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-turning-the-tables-on-cyber-attacks.pdf。

22. Lion Gu。(2014 年)。*趨勢科技資訊安全情報*。「中國行動裝置網路犯罪地下市場」(The Mobile Cybercriminal Underground Market in China)。上次存取時間 2014 年 7 月 27 日：http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-mobile-cybercriminal-underground-market-in-china.pdf。

勢科技為資訊安全軟體全球領導廠商，致力創造一個安全的資訊交換世界。我們創新的解決方案能為消費者、企業及政府機構提供多層式的內容安全防護，涵蓋行動裝置、端點、閘道、伺服器以及雲端。我們所有的解決方案皆以趨勢科技 Smart Protection Network™ 的雲端全球威脅情報為後盾，更有全球 1,200 多位威脅情報專家在背後支援。如需更多資訊，請至：www.trendmicro.tw。

TREND MICRO™

Securing Your Journey to the Cloud

趨勢科技股份有限公司
10669 臺北市大安區敦化南路二段198號8樓
電話：(02) 2378-9666
傳真：(02) 2378-0993
網址：www.trendmicro.com.tw