Internet Threats Trend Report
Q2 2010

Openfind™

commtouch®

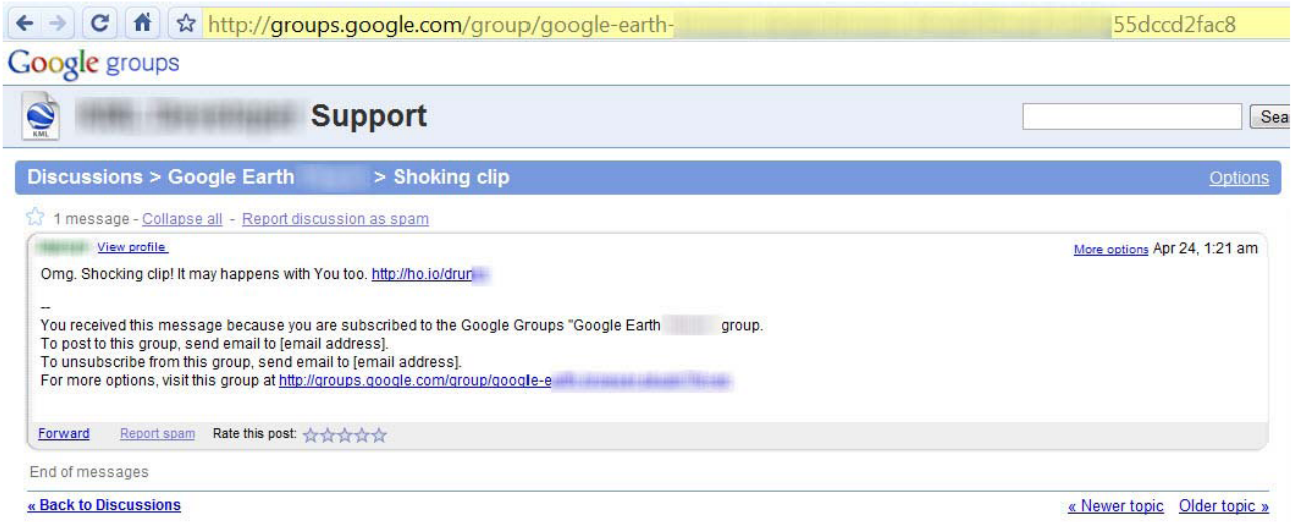
根據 Openfind 電子郵件威脅實驗室和 Commtouch 全球威脅爆發監控中心共同發表的 2010 第二季網路威脅調查報告顯示，本季中需特別注意的駭客攻擊手法，已從單純的郵件內容攻擊演變為多階段式引導的方式，透過一般使用電子郵件的三種步驟讓您受駭! 使用者需特別當心下列步驟：

1. **打開 Email**：駭客使用時下熱門的社交工程手法 (Social engineering)，讓使用者因為輕忽而打開 Email 上當
   - 重大時事：冰島火山灰事件、南非世界盃足球賽
   - 節日： 母親節
   - 知名品牌： Twitter、Apple
   - 來自似乎可信任的來源：Google Groups、Yahoo Groups
2. **有信譽的目的網站**：使用者打開 Email 後，從內容觀察，會被導引到「似乎」較具信譽的知名網站，網址包含 google、wedding wire 等，其實目的是誘導使用者重新登入其他惡意網站。
3. **當心「下一步」連結或按鈕!!**：在這樣的多階段式引導攻擊手法中，社交工程扮演了一個很重要的角色。這些網站提供了足夠的誘因讓你在多重攻擊手法中上當，像是偽裝成 Bank of America 的釣魚網站，或是想要竊取你個人資料的偽 iPhone 4 中獎網站。因此，當您在點選電子郵件裡的「下一步」連結時，請花多一點時間注意網站上的資料，以免上當!

同時，垃圾信件的發送者也大量使用免費信箱，匿名使用這些 IP 信譽等級較高的免費信箱服務廠商來發送廣告信，前三名依序為 Yahoo、Gmail 和大陸的 Sohu(搜狐)；從這些免費信箱發送出來的垃圾信連結，.ru 網域(俄羅斯)佔了其中的 26%，是十分有趣的現象。

Source: Commtouch

【利用知名品牌 Apple 發表 iPad、iPhone4 的事件，發送釣魚信件】



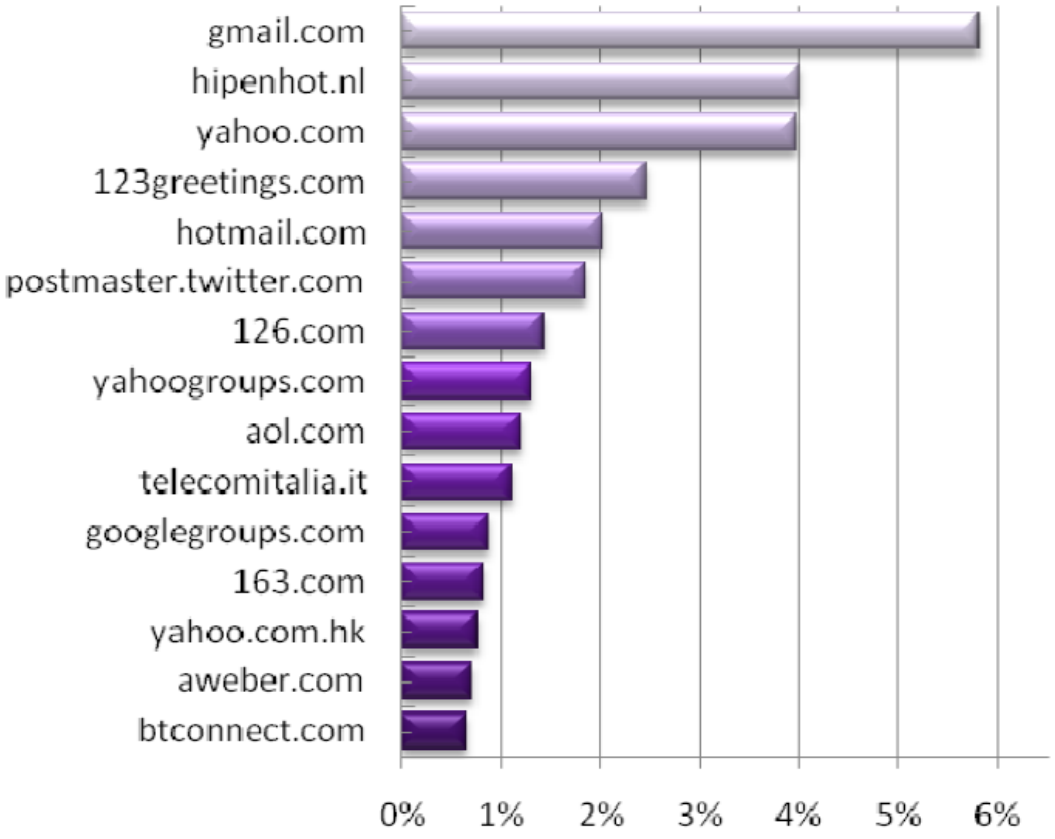
【利用 Google Groups 發送的釣魚信件樣本】

【利用南非世界盃足球賽發送的垃圾信件樣本】

2010 年第二季垃圾郵件趨勢如下：

平均每日有 1,790 億封垃圾信件流竄，Gmail 成為駭客心中假冒首選

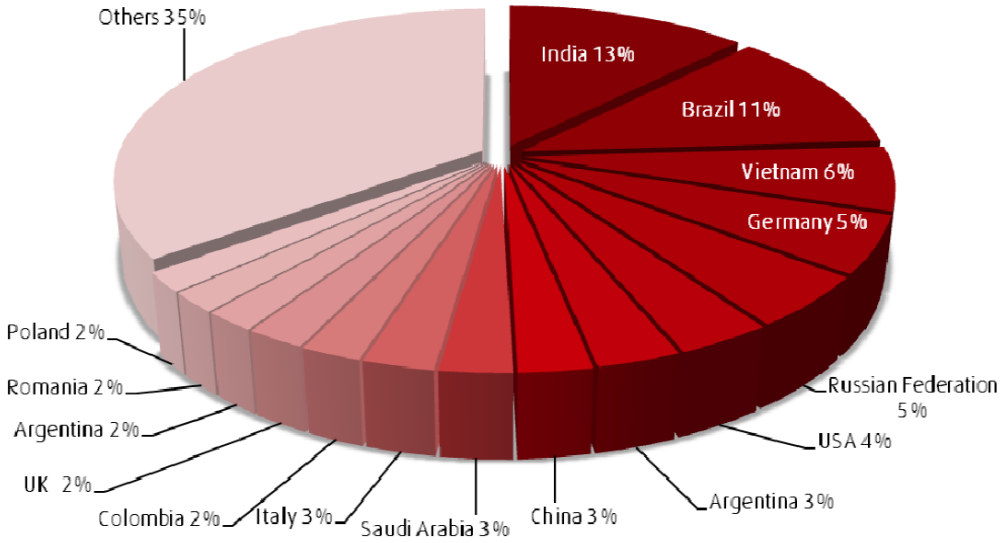
本季的垃圾郵件量仍佔了所有全球電子郵件流量的 82%，與第一季相比略為降低。而以量計算來說，每天仍有 1,790 億封垃圾郵件存在於網際網路中。這些大量的垃圾郵件，駭客最常假藉成知名網域來源，來發送垃圾郵件，其中又以 Gmail 為駭客心中首選之網域名稱。



【駭客假冒知名網域發信比率】

平均每日有三十萬七千個電腦被感染殭屍病毒

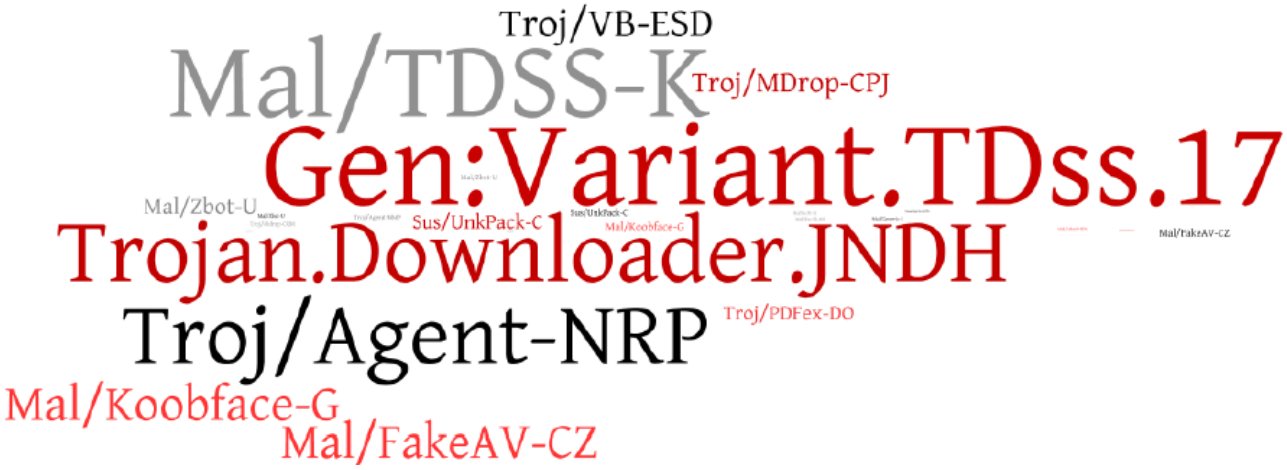
2010 第二季遭受感染的的殭屍電腦數目，比第一季的 30 萬 5 千個相比有微幅的增加趨勢。放眼世界各國，本季數據顯示印度已取代了上一季的巴西，佔了 13%，成為本季最多感染殭屍電腦的國家，其次為巴西(11%)及越南(6%)



【全球國家的殭屍電腦感染比率】

第二季惡意程式的種類趨勢

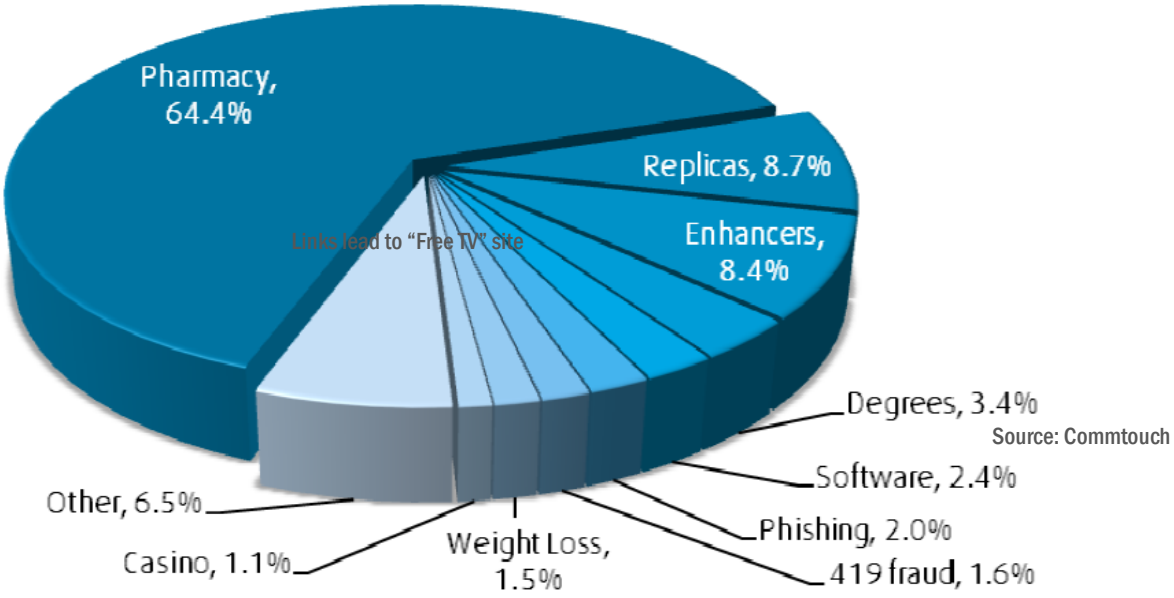
本季針對惡意程式分析結果，以標籤雲的方式呈現，其中以 Gen:Variant.TDss.17 最常出現，詐騙手法常會偽裝成微軟 Outlook 的更新檔，誘使使用者上當，其發信來源中還包含最受歡迎的偽知名網域 123greetings.com，信件內容則內夾 TDSS-K 惡意程式來攻擊使用者。此外，Mal/Bredo 惡意程式再一次的成為了惡意程式變種之王—本季共有 1,811 種，較第一季增加了 1, 000 種



【電子郵件 2010 年第二季常見的惡意程式】

藥物廣告是垃圾郵件中最受歡迎的標題 佔了 64.4%

在本季的垃圾郵件分析趨勢中指出，第二季垃圾郵件標題以藥物相關郵件仍高居第一，佔了 64.4%，但與上季報告相比則下降了 15%。此外，於本季異軍突起的垃圾郵件標題則為催情助性的藥物相關，從第一季的 2.3%攀升至 8.4%。



【電子郵件 2010 年第二季常見的郵件標題種類】

關於 Openfind

Openfind 成立於 1998 年 1 月，長期致力於網際網路相關技術研發，為企業用戶與廣大網友提供高品質、高穩定與高擴充性的軟體與服務。從企業市場搜尋引擎系列產品、電子郵件伺服器或郵件防護、加密、稽核、歸檔系統，到一般使用者的電子郵件信箱與企業郵件代管服務，Openfind 堅守「創新技術與優質服務」的企業文化，以提供使用者最符合成本效益的解決方案，更多訊息，請瀏覽公司網站 http：//www.openfind.com/。

關於 Commtouch

Commtouch Software Ltd.（納斯達克代碼：CTCH）致力於為世界上最重要的通信工具 －電子郵件，提供安全防護並保持郵件的完整性。Commtouch 在開發郵件處理軟體方面擁有超過 17 年的經驗，是全球專屬防垃圾郵件、零時病毒防護和信譽服務解決方案的全球開發者和供應商。 Commtouch 檢測中心使用包含循環樣本檢測（RPD，Recurrent Pattern Detection™）的核心技術，每週分析數十億封電子郵件，以便在新的垃圾郵件和惡意軟體進入網路網路後數分鐘內便可將其識別。眾多 OEM 合 作夥伴採用 Commtouch 技術，為遍佈全球 130 多個國家的數以千計機構的數億用戶提供保護。Commtouch 總部位於以色列涅坦亞 (Netanya)，在美國加州森尼韋爾 (Sunnyvale) 設有子公司。