Icefog 網絡間諜活動暴露

原文出處：Help Net Security (CERT 譯)

http://www.net-security.org/malware_news.php?id=2601

卡巴斯基實驗室的資安研究團隊發現了 Icefog，一個小而積極的進階持續性滲透攻擊（APT）團體。他們專注目標在南韓和日本，攻擊他們向西方公司的供應鏈。

團體於 2011 年開始運作，並在過去幾年增加了規模和範圍。

全球研究與分析團隊的主任 Costin Raiu 說：「在過去的幾年中，我們已經看到了許多的 APT 攻擊，幾乎所有類型的部門都成了受害者。在大部分的案例裡，攻擊者在企業和政府網絡內維持住一個立足點，多年下來走私出了數以 TB 計的敏感資訊。」

「Icefog ‘打游擊’ 的攻擊性質展現出一種新興趨勢：小型化的 ‘游擊戰’ 團體以外科手術般的精確度追逐著資訊。攻擊通常持續幾天或幾週，而且當他們取得他們所想要的資訊後，便會收拾乾淨打包離開。

而在未來，我們預測這種小型而專注的 ‘雇傭 APT’ 團體的數量會增加，專精於此種 ‘游擊戰’ 行動；也就是一種針對現代世界的 ‘網絡傭兵’ 」Raiu 補充。

■ 主要發現：

- 根據已辨別的目標檔案，攻擊者顯然的對以下行業有興趣：軍事，造船和海運業務，電腦與軟體開發商，研發公司，電信運營商，衛星運營商，大眾媒體和電視。
- 研究指出攻擊者針對了：國防工業承包商，如 LIG Nex1 與 Selectron 工業公司；造船公司，如大宇造船海洋科技，韓進重工；電信運營商，如韓國通訊；媒體公司如富士電視台和日中經濟協會。
- 攻擊者劫持了敏感文件和公司計劃，電子郵件帳戶憑證和密碼來存取受害者的網絡內外的各種資源。
- 在行動中，攻擊者使用 Icefog 的後門組合（也稱為 ‘Fucobha’ ）。卡巴斯基實驗室已經確認 Icefog 的版本包含 Microsoft Windows 以及 Mac OS X。
- 在其他大多數的 APT 活動中，攻擊者持續的竊取數據，而受害者保持被感染的狀態，持續數月甚至數年，而 Icefog 行動過程則是針對一個接一個受害者，找尋和複製特定的、具有針對性的資訊。一旦獲得了所需要的資訊，他們就會離開。

- 在大多數案例裡， Icefog 行動顯示了他們非常清楚地知道他們需要從受害者身上得到什麼。他們尋找特定的文件名，很快地識別，並轉移為C&C(命令與控制)攻擊。

■ 攻擊和功能：

卡巴斯基研究人員已經捕捉攻擊者所使用的 70 個以上的網域中的 13 個。這提供了全世界受害者的統計數量。此外，Icefog 的 C&C(命令和控制)伺服器保持的加密日誌記載著受害者在它們上面執行的各種操作。這些日誌有時可以幫助識別攻擊的目標，並在某些情況下，找出該攻擊的人。

除了日本和南韓，許多陷阱連結也在其他幾個國家進行了觀察，包括台灣，香港，中國，美國，澳大利亞，加拿大，英國，義大利，德國，奧地利，新加坡，白俄羅斯和馬來西亞。

總體而言，卡巴斯基實驗室觀測到超過 4000 個獨特的感染 IP 和幾百個受害者(數十個 Windows 的受害者和超過 350 個 Mac OS X 的受害者)。

根據名單上的用於監視和控制基礎設施的 IP 位址，卡巴斯基實驗室的分析師假設了這些威脅行動背後的人員都至少來自這三個國家：中國、南韓和日本。