惡意程式-Flame 簡介

目錄

前言

與 Duqu 相同，Flame 並不是「一個」程式，它是很多模組包在一起的一個惡意攻擊工具組，約 20MB 大小，由於主要負責攻擊和感染的模組叫做 Flame，卡巴斯基實驗室便以此命名（也有其他單位稱它為 SkyWiper 或 Flamer）

Flame 比 Stuxnet 大二十倍，也比 Duqu 要複雜。關於 Flame 截至目前為止仍有很多不清楚的地方，比如初始傳染的載體為何，我們懷疑它可能是利用漏洞，或是什麼特別的針對式攻擊。

一旦 Flame 成功感染目標主機，它會展開一連串複雜的行動，包括監聽網路流量、畫面截圖、錄下語音對話…等。所有被 Flame 感染的主機的資料，Flame 的 C&C 都可以透過它得到。Flame 背後的操作者還可以上傳更多的模組，拓展 Flame 的功能，約有 20 個模組，而多數模組的功能還在調查中。

Flame 一開始怎麼感染電腦的？

Flame 有兩個專為感染 USB 的模組：「Autorun Infector」和「Euphoria」，但是並未看到這兩個模組活動，或許是因為在設定檔裡面為 disable 狀態。不過，感染 USB 的能力確實在 Flame 的 code 裡面出現，它使用了兩個方法：

- Autorun Infector：來自於 Stuxnet 的「Autorun.inf」，它利用 shell32.dll 進行感染，而這種方法只在 Stuxnet 見過。
- Euphoria：利用 LNK 檔，使得使用者點擊進入資料夾時，即被感染。而該資料夾名為「junction point」。

此外，Flame 也可以透過 LAN 傳播：

- 利用具有 MS10-061 漏洞的印表機，Stuxnet 也使用此漏洞
- 遠端工作
- 當 Flame 被擁有網路管理員權限的使用者執行時，便會開始在網路上面攻擊其他電腦，它透過網路在其他主機上面創造具有預設密碼的後門帳

號，接著把自己拷貝到該主機上面

在 Flame 上並未看到像 Stuxnet 使用多個未發布的漏洞攻擊，它主要仍是透過網路攻擊已達至最新更新狀態的 Windows 7 主機。

為什麼 Flame 這麼複雜？

Flame 裡面包含了許多函式，提供許多功能：壓縮（zlib、libbz2、ppmd）、資料庫操作語法（sqlite3）等。某些部份的 Flame 程式碼用 Lua 寫成，Lua 是一種腳本語言，可以輕易地被擴展。Lua 只佔的 Flame 程式碼的一小部份，約 3000 行。

由於 Flame 程式碼的龐大，使得執行和除錯變得很困難，Flame 不僅不是一個傳統的可執行程式，它的某幾個 DLL 檔還會在系統開機的時候自動載入。因為上述原因，Flame 可說是目前為止已發現的最複雜的威脅之一。

Flame 和其他的後門程式有何不同？

Flame 使用 Lua 這個腳本語言整合和拓展其功能，惡意程式使用 Lua 很不尋常，多數惡意程式為了隱藏容易，通常以非常簡潔的程式碼實作，而且都很小，鮮少像 Flame 有 20MB 這麼大。

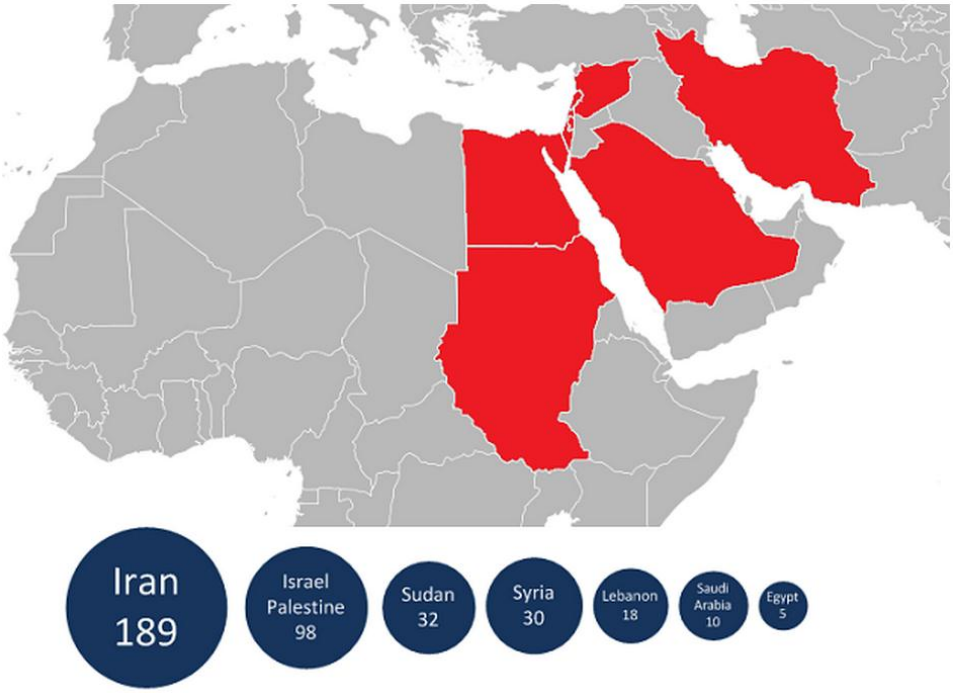
Flame 可以紀錄語音資料也很少見，雖然這不是很難的事，但是 Flame 竊取資料的多樣性卻是前所未見。Flame 將語音錄製起來之後，透過公用的函式庫壓縮並儲存。接著這些資料會透過隱藏的 SSL 頻道傳送到 C&C 去。

Flame 有固定擷取螢幕畫面的能力，更甚者，Flame 是在某些它有興趣的應用程式啟動時才會開始擷取螢幕畫面，一樣透過函式壓縮之後儲存固定回傳給 C&C。

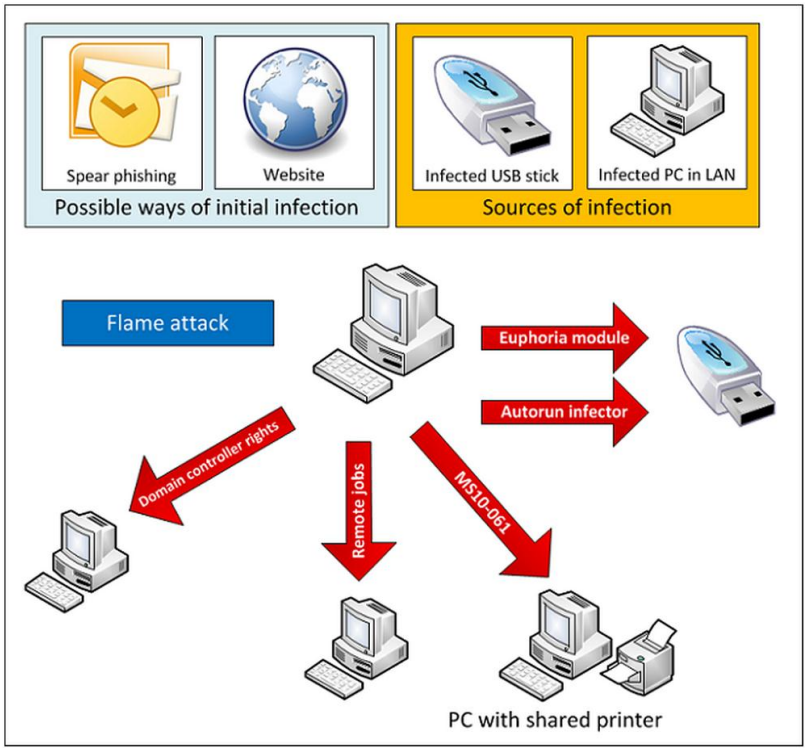
Flame 背後的謎

目前已知有三個可能研發 Flame 的團體：國家、網路犯罪集團、駭客激進團

體（hacktivisits）。Flame 不是設計來竊取銀行資料的，它也和常見的惡意程式有很大的不同。由於 Flame 感染目標的地理位置特殊，以中東國家為大宗，所以背後的研發團體最有可能是一個國家。



圖為 Flame 感染的國家：伊朗最多、以色列次之，接著是蘇丹、敘利亞等中東國家



Flame 在感染成功之後，會監控連線狀態、攻擊其他電腦的成功次數等，雖然 Flame 不像 Duqu 和 Stuxnet 擁有計數器而能夠自我毀滅，但是遠端的攻擊者可以傳送一個特別的模組 browse32，使得 Flame 能完整解除安裝。

參考資料

http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers