惡意程式-Duqu 簡介

目錄

前言

Duqu 並不是「一個」惡意程式，它由一些元件組成，一起共同進行惡意活動。許多安全單位都發布了關於 Duqu 的分析，每個單位發布的分析結果在細節上有所不同，但是大概念是相同的，以下的敘述主要參考 Kaspersky 所發布的報告。

Duqu 的組成

Kaspersky Lab 將 Duqu 分為兩個部份：主要模組和一個 keylogger

主要模組含有三個部份：

- 可以將 DLL 注入系統行程的驅動
- 含有可以與 C&C 互動的額外模組的 DLL
- 設定檔

Keylogger 則是一個獨立的鍵盤指令紀錄器，和主要模組一起在受害電腦上被發現，主要模組擁有下載其他元件的能力，所以我們假設它們彼此在某種程度上是有相關的，或者說，我們認為 Keylogger 是主要模組被安裝之後下載的。Keylogger 將蒐集到的資料存放在類似「~DQx.tmp」的檔案裡面，這也是 Duqu 命名的由來。

Keylogger 作為一個 Trojan-Spy，可以獨立運作；當然，主要模組也可以獨立運作不需要 Keylogger，兩者之間的關聯並不是如此的明顯，

怎麼發現 Duqu 的？

2011 年 9 月 1 日，一個名為「~DN1.tmp」的檔案從匈牙利的某個電腦上被送到 Virustotal 上掃描，當時被四個防毒軟體偵測到。這是防毒軟體公司第一次認識 Duqu。這個被送到 Virustotal 掃描的檔案是前面提過的 Keylogger。我們可能會認為，既然有防毒軟體可以認出 Duqu 的部份，那顯然 Duqu 的作者對於讓 Duqu 免於偵測並不是很上心，所以 Duqu 的主要模組被偵測到也是遲早的事。

不過事情並不是我們所想的那樣。2011 年 9 月 9 日，Duqu 的主要模組，以

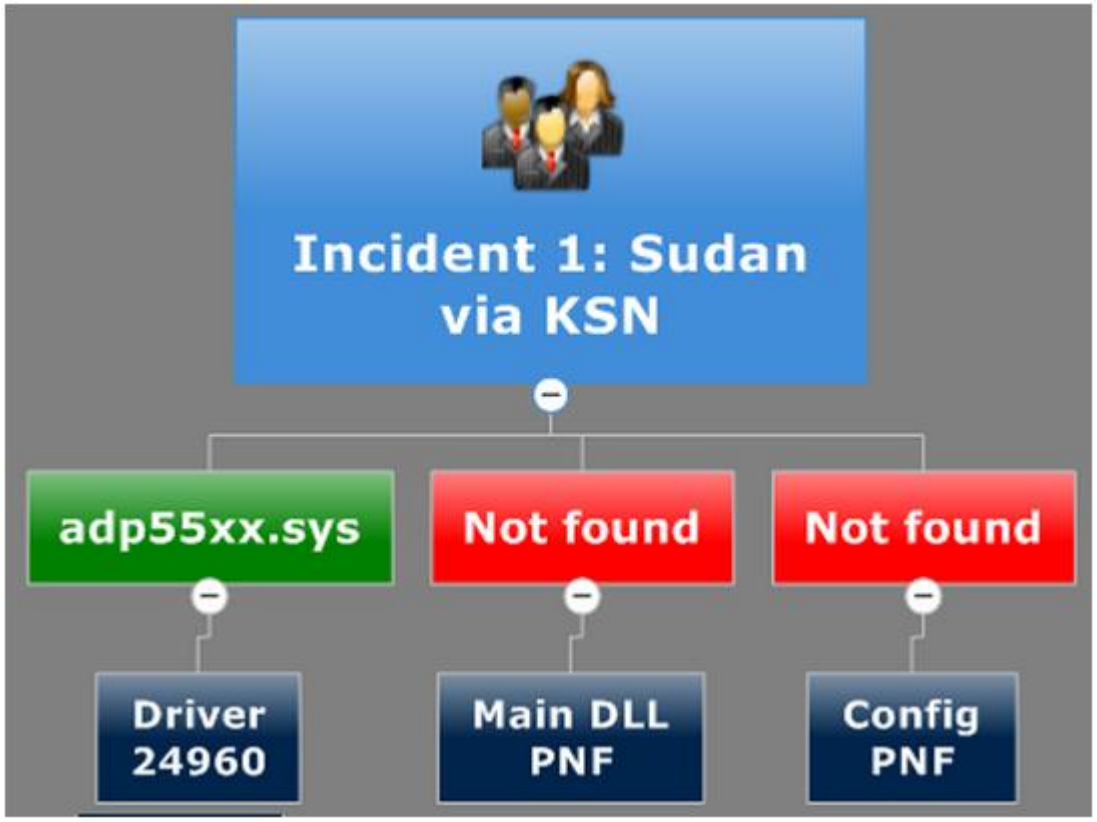
「cmi4432.sys」的檔名在同樣的國家被上傳到 Virustotal，cmi4432.sys 具有 C 數位媒體公司的簽章，是一個主機板音效驅動程式，當時沒有任何一個防毒軟體偵測到它的不尋常，Duqu 的作者非常精心地製造了它，即使我們後來發現它和 Stuxnet 有相似之處，但明顯的，Duqu 的作者改寫了程式碼，使得 Duqu 主要模組無法被防毒軟體偵測。

2011 年 9 月 18 日，另一個檔名為「jminet7.sys」被上傳到 Virustotal，另外一個驅動程式，當然也沒有任何防毒偵測到。之後，Duqu 的主要模組一直以驅動程式的樣子出現變種，它們的大小、檔名、MD5 都不相同，這表示 Duqu 的作者密切關注這些。

實際案例

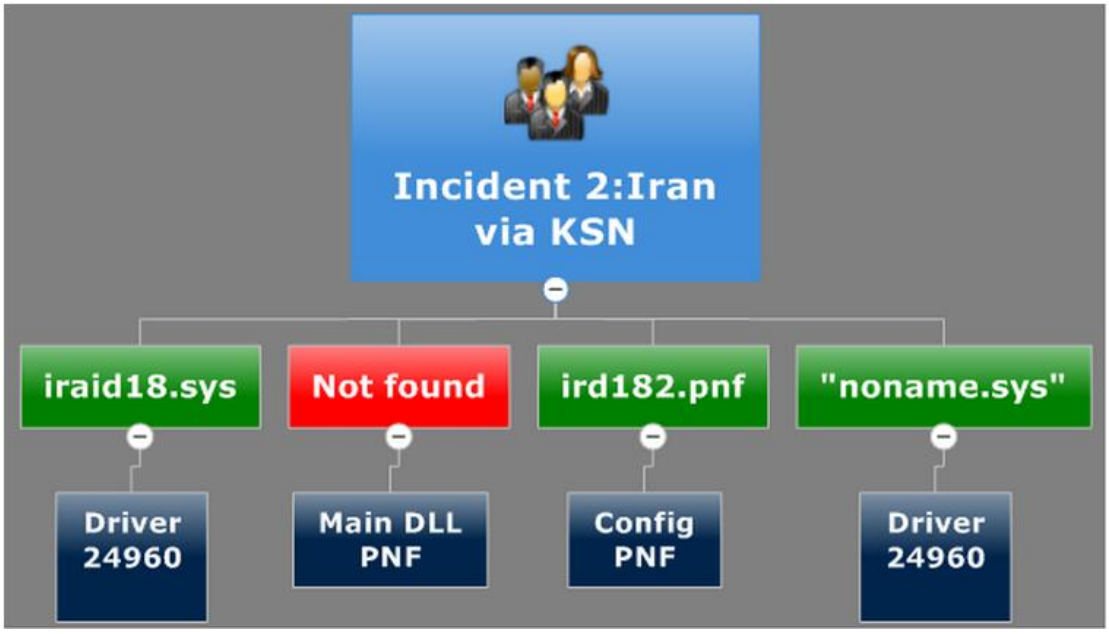
即使早期上傳到 Virustotal 的 Duqu 來自匈牙利、澳洲、印尼等，在實際的案例中，以伊朗的活動最多，我們認為 Duqu 分佈了整個世界，但是只有在伊朗的最為活躍，這表示 Duqu 有特定的攻擊目標。

#1 地點：蘇丹



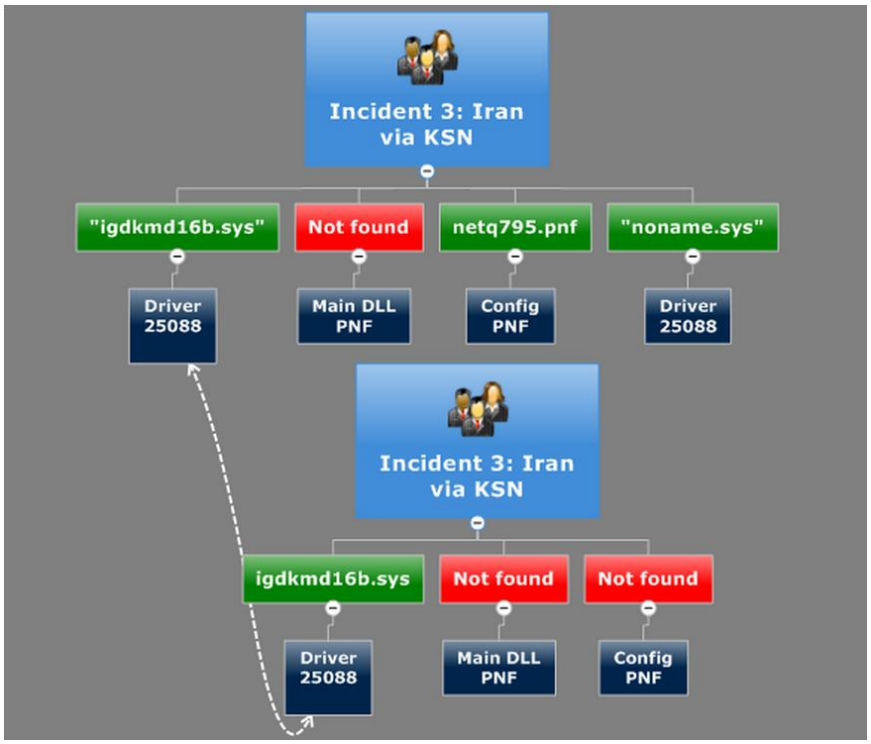
我們僅發現主要模組中的驅動元件「adp55xx.sys」，而 DLL 以及 Config 並沒有偵測到，這意味著，這個案例裡面的 DLL 以及設定檔可能不同於我們已經知道的例子，所以才沒有被發現。

#2 地點：伊朗



伊朗是 Duqu 案例最多的地方，和先前有相同的模式，又一個不同的驅動名稱「iraid18.sys」，大小和「adp55xx.sys」相同，MD5 不同。Config 檔也是已知的大小，不過內容稍有不同，使得 MD5 也不同。有趣的是這個案例中發現了另外一個驅動（noname.sys），和先前看過的完全不一樣。

#3 地點：伊朗



這次的案例是一個彼此連接位在同一個網路的兩個系統，它們被同一個驅動感染「igdkmd.sys」（沒看過的檔名、大小、MD5），在其中一台電腦上面發現了 Config 以及另外一個驅動。

結論

- 很明顯的，每一個案例發現的驅動名稱和 MD5 都不一樣，大小有時候會相同
- Duqu 在針對性攻擊中被使用，攻擊目標經過精心挑選
- 至少知道有 13 種不同的驅動存在
- 在分析「igdkmd.sys」時發現一把新的加密金鑰，這表示目前已知偵測 DLL 的方法是無效的，而每一個案例中的 DLL 都個別加密過。目前所有的防毒都可以偵測到 Duqu 的主要驅動元件，對特別加密過 DLL 卻不是如此
- DLL 檔可以重新設置安裝，它能夠安裝驅動並且生成額外的元件，如果它與 C&C 有連結，Duqu 在每個系統上的元件架構可能都不會相同。
- 有些報告說 Duqu 只感染系統 36 天，這不盡然正確。只有某幾個例子真的有達到 36 天，有一些則在 30 天後就把自己移除掉了。

參考資料

http://www.securelist.com/en/blog/208193182/The_Mystery_of_Duqu_Part_One
http://www.securelist.com/en/blog/208193197/The_Mystery_of_Duqu_Part_Two