臺灣大學計資中心網路組

北區學術資訊安全維運中心

資訊安全分析報告

BOT: H-Worm 惡意程式檢測與修補

臺灣大學計資中心網路組

北區學術資訊安全維運中心

目錄

摘要

H-Worm 是北區 ASOC 轄下台北區網中心近期偵測數量最多的惡意行為。本報告說明 H-Worm 惡意程式的特徵及影響，並闡述北區 ASOC 檢測與分析 H-Worm 惡意程式之行為，以及提供使用者防範及移除此惡意程式的方法。

H-Worm 惡意程式簡介

蠕蟲(Worm)與病毒(Virus)相似，是一種能夠自我複製的電腦程式。與病毒不同的是，蠕蟲不需要附加在任何程式內，也不需要使用者操作就能夠自我複製或執行。

病毒的攻擊方式大多是直接破壞受感染的系統。蠕蟲雖然也會毀損或修改主機內的檔案，但它們大多仍採取分散式阻斷服務攻擊(DDoS)的方式，塞爆目標主機的網路頻寬，降低目標主機的執行效率，進而影響主機的正常使用。[註 1]。

而 H 型蠕蟲(H-Worm)是一個以多種途徑散播的惡意 VBScript 程式。當使用者未注意或不小心開啟受感染的電子郵件時，蠕蟲立即被執行，搜尋特定的檔案類型並修改或覆寫檔案內容。由於 H-Worm 的程式碼採取的攻擊方式為覆蓋或修改而非刪除該檔案，所以在檔案的復原上相對困難。

而 H-Worm 還有一個特性，從已經被殭屍網路(botnets)感染控制的主機當中，優先挑選可以加快攻擊規模或速度的主機使用，以便提升攻擊與感染之效率。

H-Worm 惡意程式的影響

H-Worm 除了可以進行簡單的遠程命令與操作外，攻擊者也可遠程快速升級殭屍電腦(Bot)功能，提前在系統修補漏洞之前進行攻擊。典型的 Bot 活動包含攻擊者從這些受攻擊的系統中，下載新的攻擊模組以獲取敏感訊息（例如 Windows serial number, AOL account 等等），並利用這些受感染的系統對其他系統進行 DDoS 攻擊。

H-Worm 惡意程式的特徵

H-Worm 惡意程式具有以下的特徵：

1. H-Worm 進行網路活動時的封包內容可能包含下列關鍵字：

- /is-sending
- /is-recving
- /is-enum-driver
- /is-enum-process
- /is-cmd-shell
- /is-ready
- \x3c\x7c\x3eplus\x3c\x7c\x3e
- \x3c\x7c\x3eunderworld final\x3c\x7c\x3e

2. 封包內容可以觀察到受感染的主機，會透過 HTTP 方式向特定 C&C Server (Command and Control Server)回報：

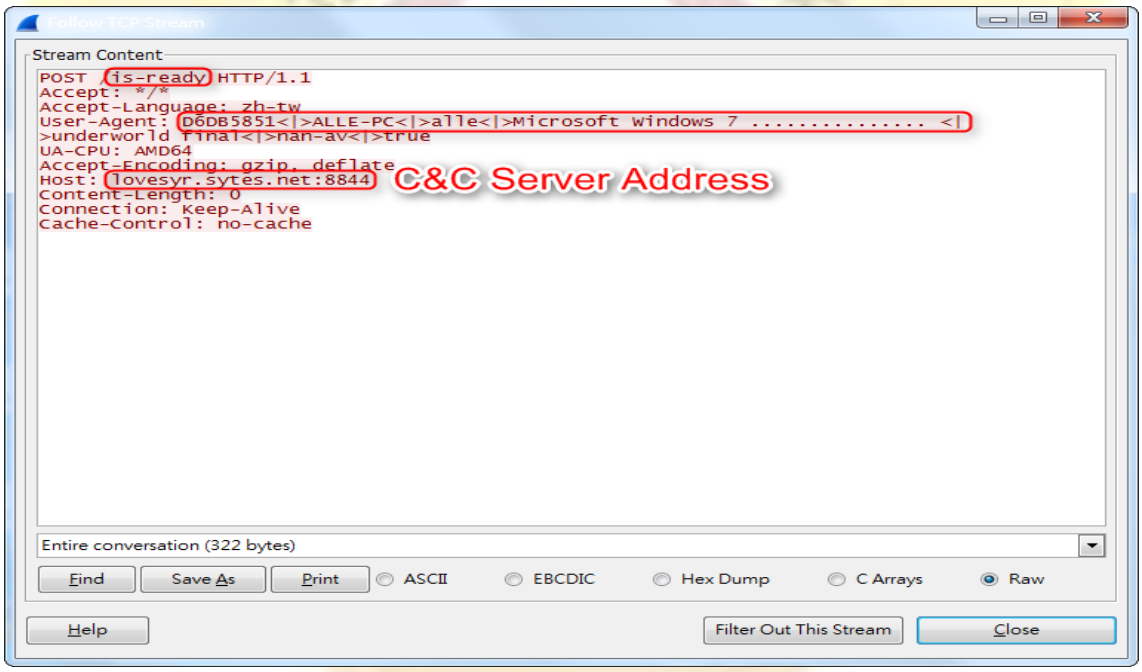

圖 1 案例封包中受感染主機透過 HTTP 方式向 lovesyr.sytes.net:8844 進行回報

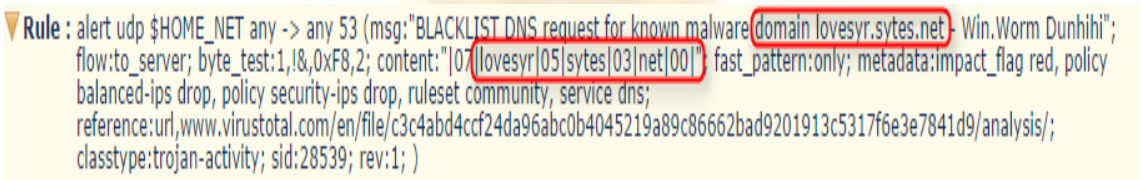

圖 2 此 snort rule 為偵測感染 H-worm 後，向特定惡意 domain 查詢

H-Worm 惡意程式可能造成的危害

為了瞭解感染此惡意軟體後與 C&C Server 間的互動，我們在作業系統 Windows 7 Professional 64 位元的 VM 環境下進行實測。從圖 3 中可以發現，受感染的主機其 Client ID、Computer Name、User Name 及 Operation System 相關訊息皆會出現在其清單內，從圖 3、圖 4 中可以發現攻擊者除了可以使用此惡意程式中的 process list 功能隨時更新(refresh)受感染主機的工作清單，也可以隨時停止(exit process)正在執行的工作程序。

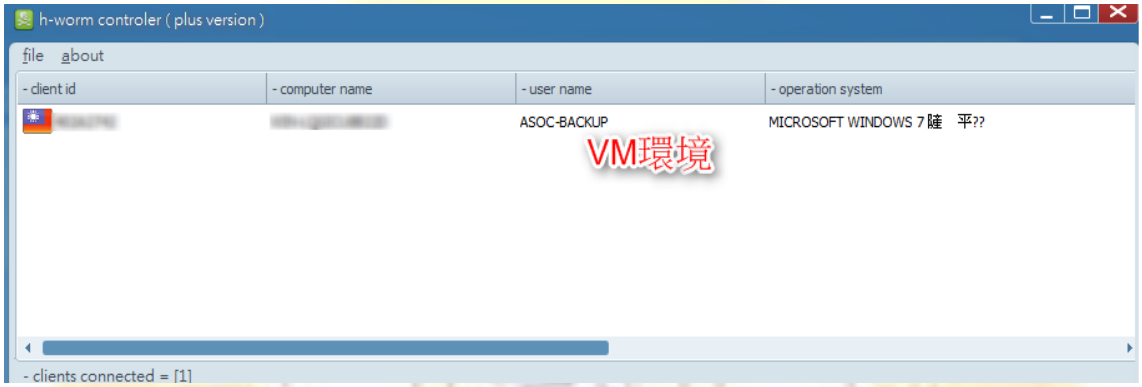

圖 3 受感染的主機清單

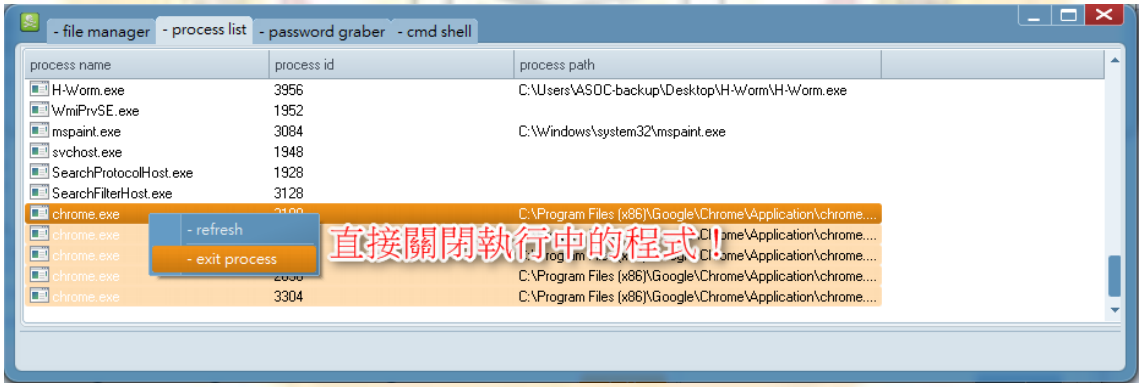

圖 4 更新或關閉 process list 中的程序

從以下圖 5、圖 6 顯示攻擊者可以任意瀏覽受感染主機的硬碟，並可下載惡意程式，也可以上傳想要竊取的檔案。如果攻擊者沒有上傳與下載任何資料，也可以選擇直接刪除感染主機的任意資料以達到破壞之目的。

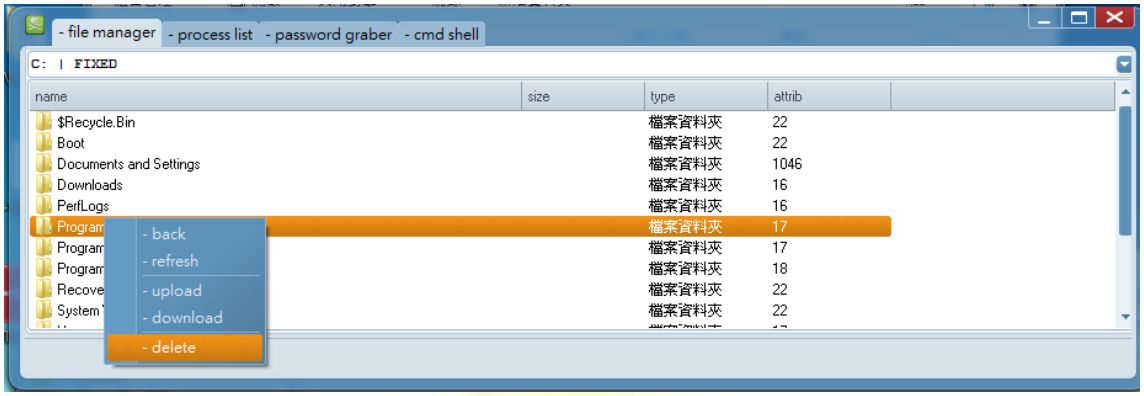

圖 5　檔案資料的管理

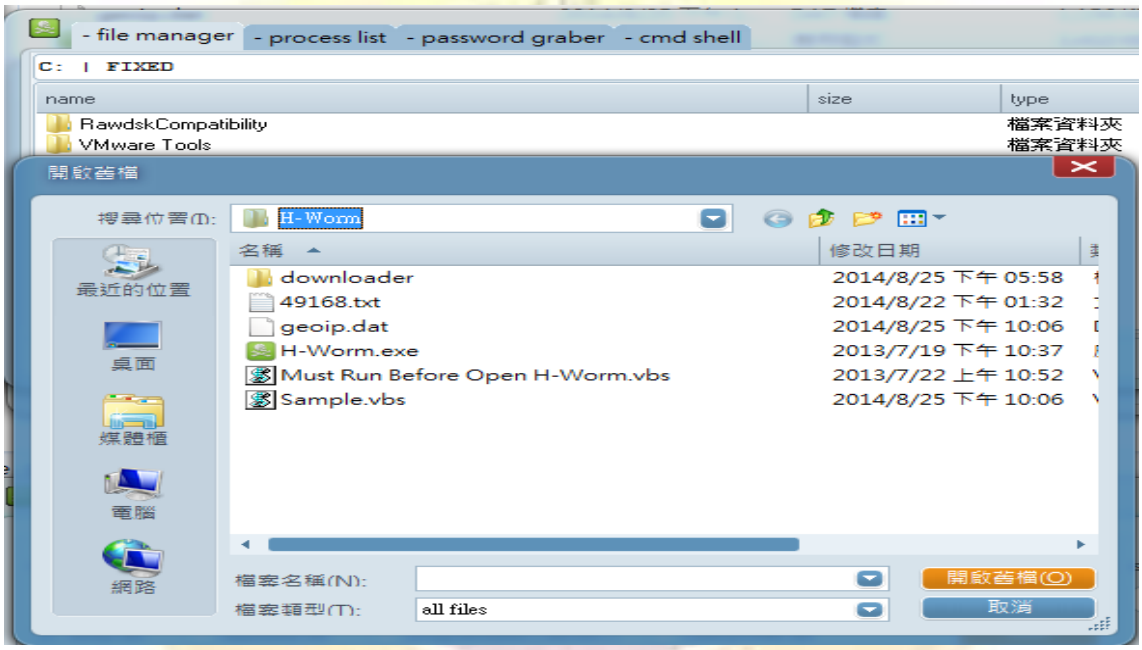

圖 6　上傳與下載資料

除了上述的簡易指令可以達到某種程度的破壞或危害之外，此惡意程式包含了 cmd shell 攻擊方式。可以執行遠程的 Command 指令，這些指令包含了直接關機(shutdown -s)或重新開機(shutdown -r)等。

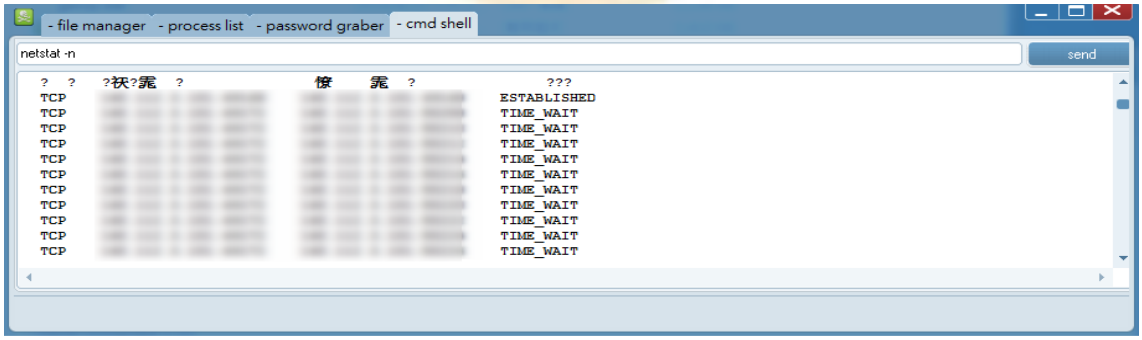

圖 7 執行遠程的 Command 指令

如何防範 H-Worm 惡意程式

主機在下列情況下容易遭受 H-Worm 惡意程式感染：

1. 未安裝防毒軟體於電腦主機或防毒軟體已失效。
2. 使用非法或來路不明的軟體。
3. 沒有定期更新作業系統。
4. H-Worm 的攻擊途徑大多經由電子郵件，所以缺乏對郵件社交工程攻擊的了解與認識也是一大原因。

該如何防範 H-Worm 惡意程式，應落實以下使用行為：

1. 確保防毒軟體的安裝與使用功能正常。
2. 不使用非法或來路不明的軟體，任何可疑檔案皆須經由防毒軟體掃描後使用為妥。
3. 務必落實作業系統之更新。
4. 開啟電子郵件的附件或點擊電子郵件中的連結，皆須審慎為之。

※ H-Worm 的防毒軟體偵測率非常高，務必落實防毒軟體的防護與掃描。

如何檢測及移除 H-Worm 惡意程式

關於 H-Worm 的檢測，首先我們在 virustotal 上傳受感染的樣本檔案(SHA256:a6bd7ae00b55b684c10e7c708b00ce46b091115fc0e4d2d8bc3e415b5dfca496)，可以發現它被偵測到的機率非常高(圖 8)(樣品 81c153256efd9161f4d89fe5fd7015bc 和 4543daa6936dde54dda8782b89d5daf1 也是 H-Worm 的樣本)。

我們針對 H-Worm 的檢測所使用的防毒軟體為 Microsoft Security Essentials，使用此套工具，我們可以偵測並移除惡意的文件資料，該如何檢測及移除 H-Worm 惡意程式，於下方步驟中說明：

圖 8　H-Worm 於 virustotal 的偵測結果

對於 H-Worm 蠕蟲的檢測及移除方式我們傾向於防毒軟體的落實。以下用 Microsoft Security Essentials 防毒軟體說明：

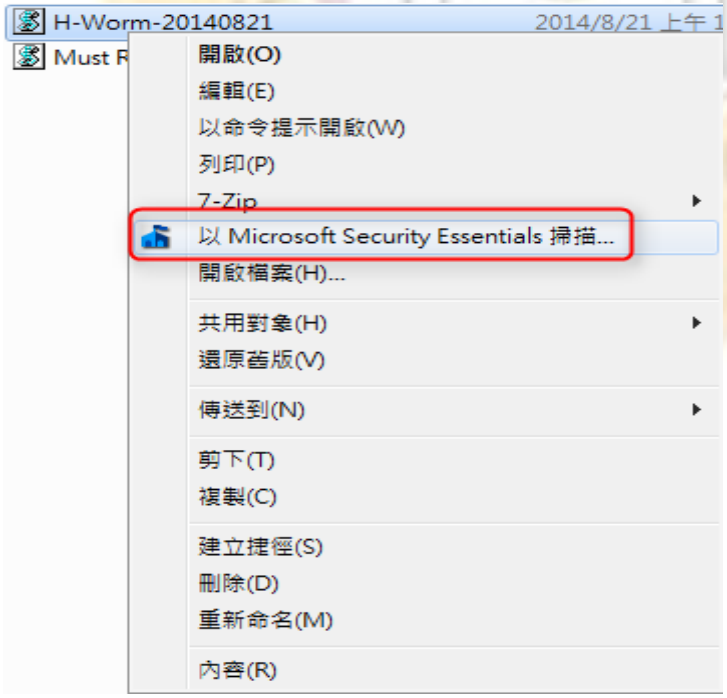

圖 9　主機檔案掃描

圖 10　H-Worm 的防毒軟體偵測率非常高

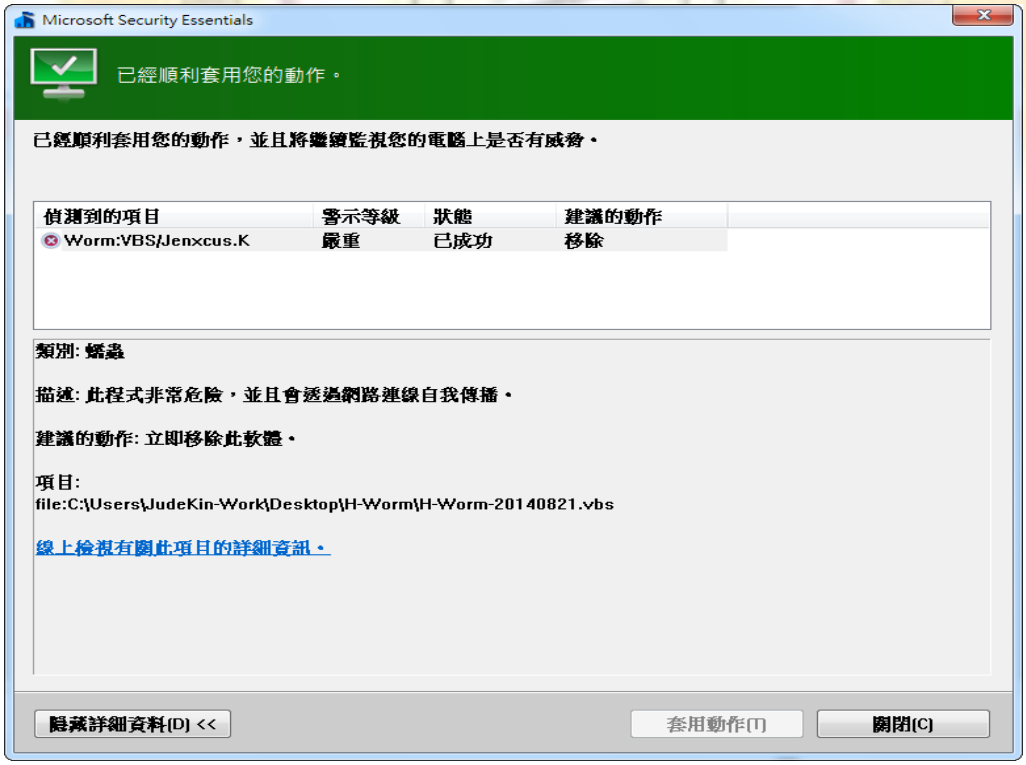

圖 11　移除 H-Worm 惡意程式

參考資料

[註 1]
引自 Wikipedia，
http://zh.wikipedia.org/wiki/%E9%9B%BB%E8%85%A6%E8%A0%95%E8%9F%B2
[註 2]
引自 FireEye，
http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/now-you-see-me-h-worm-by-houdini.html
[註 3]
https://www.virustotal.com/zh-tw/