偵測聯合攻擊之研究

陳嘉玫
中山大學資訊管理學系
cchen@mail.nsysu.edu.tw
蕭漢威
高雄大學資訊管理學系
hanwei@nuk.edu.tw
李宗南
中山大學資訊工程學系
cnlee@cse.nsysu.edu.tw
楊中皇
高雄師範大學資訊教育研究所
chyang@nknucc.nknu.edu.tw
楊鵬宇
中山大學資訊管理學系
M994020007@student.nsysu.edu.tw

摘要

網路安全在惡意攻擊與偵測防禦的領域上相互較勁已經持續多年，近年來隨著資訊技術的發展，許多網路惡意攻擊事件由原先的單一攻擊來源，進化成為自動化而具智慧型的多點聯合攻擊模式，這類的模式大多由殭屍網路所發動。本研究發現一種有別於以往來自單一主機的攻擊手法，新的攻擊手法聯合殭屍網路內的其他機器進行合同攻擊，用以規避以往的偵測模式。本研究針對此種偵察者與侵入者聯合攻擊，根據攻擊的手法訂定隱藏序列以及其對應的特徵，以隱藏式馬可夫鏈進行模型的建立與調整，並以此對殭屍網路的攻擊進行偵測，增加防範的能力。

關鍵詞：殭屍網路、隱藏式馬可夫鏈、入侵偵測系統

壹、緒論

近二十年的時間中，網際網路飛快的發展，隨著電子處理與儲存設備的進步與成本降低，全世界連接上網的使用者人數迅速的增加(Castells 2009)，電子商務商機愈發蓬勃發展，隨著交易量與金額增加，相關資訊盜竊所帶來的不法利益也隨之升高，使用者於交易中的資訊遭到網路罪犯的竊取，繼而用來進行不法的交易，或是用來進行相關的詐騙行為以謀取利益。企業彼此間的競爭也可能涉及的網路上的機密資訊竊取，並以惡意攻擊手法，例如阻斷服務攻擊的手法試圖使對手的服務中斷(Shadowserver 2005)，藉此來造成對手的損失。隨著網路基礎設施的演化，相關服務提供廠商的負載能力提升，單一主機所發動的阻斷服務攻擊難以有效干擾網路服務，為了能夠創造大量數據流量以使目標癱瘓，網路罪犯需要大量主機同時發動攻擊，主機的數量常常達到數以萬計之譜，包含如此巨量主機的群體不論是新增受到感染的主機或是對主機群進行管理，都是相當難以進行的動作，所以為了能夠自動化的感染並管理主機群，同時又能兼顧匿蹤的特性，網路攻擊技術已往自動化的方式發展，其中最具代表性並且影響層面最大的即是殭屍網路(Botnet)，殭屍網路是一個由受感染的主機群，與命令發佈控制主機(Command and Control – C&C)組成的群集。殭屍網路操控者(Bot Herder)透過 C&C 主機發佈相關攻擊指令，對特定目標於設定的時間範圍內發動攻擊，干擾目標服務提供，造成目標廠商的損失等模式進行商業上的競爭。根據 H-online 的報導，去年八月時德國境內的房地產經銷商與食物外送服務網站，都受到了分散式阻斷服務攻擊，造成相關外送服務的癱瘓(The H-security 2011)。

殭屍網路(Botnet)已經成為最為廣泛使用的一種惡意程式執行架構，具有自我擴散的能力，藉由列舉出受害者所運行的程式，以及使用相對應該程式的弱點攻擊手法，殭屍網路得以對受害者進行攻擊，並於感染受害者後取得受害電腦的控制權，將自己隱藏起來，並於需要時被攻擊者以特定的方法喚醒，執行被指定的任務。

因為殭屍網路具有高度自動化的特性，經過調整與校正過後，往往很輕易的就可以自動進行感染與傳播，兼之攻擊者經常會不停的對攻擊程式進行修改與增加新的攻擊技巧，故殭屍網路內的感染電腦數量通常會迅速增加且數量驚人。

近年來，在許多的學者與資安人員不間斷的努力下，與駭客的攻防拉鋸戰中，在針對單一攻擊的入侵偵測系統已經大有斬獲，但是近來發現一種新型態的聯合入侵攻擊模式已

經成為新的殭屍網路進行入侵的主要手段。此一類型的攻擊模式包含了兩台以上殭屍電腦進行搭配組合的入侵攻擊，能夠對現有針對單一連線的偵測方式做出有效的規避，使之失準。

新型態的殭屍網路聯合入侵攻擊模式首先會以剛被感染的電腦進行大量密集的掃描，並對網域內的其他主機進行暴力密碼破解，此類電腦本研究稱為 “偵察者”(Scout)，因其主要工作為探測目標主機之防禦漏洞。在成功的試出受害者特定的服務所使用的帳號與密碼後，將掃描結果藉由電子郵件寄回予攻擊者，再以殭屍網路中的其他電腦進行正常登入，此類電腦本研究稱為“侵入者”(Striker)，因為已經取得目標電腦的弱點，故此類電腦的攻擊手法常是一擊中的。此種攻擊手法的好處是一來目標主機雖然會注意到進行暴力破解之”偵察者”，並有可能對其做防範動作，像是列入黑名單或是列入高價值觀察對象，但是另一個首次登入就以正常帳號密碼組合的“侵入者”主機來源，就會被目標主機視為正常登入，而輕易放行，使得相關的偵測機制無法進行偵測，進而使攻擊者達到規避一般主機防禦系統的功能。

此一攻擊手法與利用低頻率的掃瞄與密碼破解攻擊目的極為類似，由於偵測系統需要藉由單一主機進行密集的連線次數來進行異常偵測決定是否遭受攻擊，故當攻擊模式是分散式的攻擊，就可以避免系統有留下明顯的攻擊特徵，藉以規避系統偵測。

傳統偵測方法遇到新型態的攻擊時可能遇到下列不同的問題：對於網段內各個主機進行探測掃瞄與帳號密碼破解的外來 IP 位址，網路入侵偵測系統(NIDS)可以輕易的偵測出來，但是，相對於在其後以掃描探測結果進行正常登入的主機，因為在流量偵測系統中被定義正常行為，故不會被流量偵測系統發現。至於針對主機內部的異常行為進行檢測的主機異常偵測系統(HIDS)，所在意的是各種軟體與資源的異常存取以及權限的違反，一旦相關的攻擊於剛入侵時，取得了管理者的權限，則入侵者可將 HIDS 的偵測機制關閉，使之無效，則相關的偵測機制也就付之闕如，失去原本的效用了。故能夠得知，相關的傳統偵測方法在遇到新型態的偵察者與侵入者聯合攻擊時，無法有效的發現相關的攻擊訊息。

本研究目標在於偵測新型態的殭屍網路攻擊，希望以隱藏式馬可夫鏈(Hidden Markov Chain)找出正常使用以及偵察者與侵入者聯合攻擊模式所留下軌跡之間的差別，並以此協助補強傳統偵測方法無法偵測到的異常行為。

貳、相關研究

攻擊者使用惡意程式對他人的電腦進行感染，將後門或是遠端操控系統植入受害者的電腦內，受害者的電腦即會像是殭屍或是傀儡一般的受人擺佈，藉由 C&C 伺服器做為中介的溝通模式，攻擊者得以對龐大的殭屍電腦軍團發佈各種指令，此種電腦構成的網路群組，即稱為殭屍網路，也就是所謂的 Botnet。殭屍網路已經是現在各種網路犯罪的主要管道，從阻斷式攻擊到廣告郵件散佈，因為殭屍網路本身龐大的運算節點、運算能力以及龐大頻寬，經由殭屍網路發起的攻擊往往能造成網站癱瘓、服務中斷。這個龐大的犯罪系統當然不是一個兩個人可以維護或是建置的，所以在殭屍網路內部可以觀察到分工的跡象。

殭屍網路的建立，從攻擊者取得殭屍程式，在成功的潛入受害者的電腦後，根據預先設定好的 IP 位址進行遠端控制。此後以惡意網路郵件、或是藉由針對特定程式的弱點攻擊進行自動擴散，並於控制受害者電腦後進行回報，以此建立一個基本的殭屍網路架構。

Li 等人(2009)的研究指出，待殭屍網路達到一定規模後，攻擊者此時會開始進行出租殭屍網路電腦的行為，根據買家欲使用的殭屍數量、攻擊目標、手法與時間長短來進行收費。例如出租給其他使用者散播其廣告郵件發送程式，使用者得以發送大量的廣告郵件，藉此牟利。或是出租電腦，供他人做代理伺服器，在 2011 年 9 月，Kerbs on Security (2011)報導資訊安全人員發現有攻擊者使用一個被稱為 TDSS 的殭屍程式建立殭屍網路，並建立網站 awmproxy.net，該網站專營出租代理伺服器的業務，根據出租的時間長短以及電腦數量計費。根據所提供的服務有所不同，殭屍網路控制者可以從經營殭屍網路而收取到不同數量的金錢。而不論是進行殭屍網路租借的使用者或是撰寫殭屍程式攻擊者，都可以從中謀利，賺取金錢。以殭屍網路為骨幹，網路犯罪也有自己的經濟行為，具有強大程式撰寫能力的攻擊者負責製造新的惡意程式，增加新的功能以躲避防毒廠商以及各地資訊安全人員的偵測，並將此類程式販售給經營殭屍網路的攻擊者。攻擊者利用相關的工具建置殭屍網路後，再出售殭屍網路所提供的運算服務。各式各樣的顧客則跟攻擊者買相關的服務，從阻斷式攻擊、資訊竊取到散播惡意程式不一而足，並從此類惡意行為所帶來之效果獲利。

Gu 等人(2007)將攻擊者入侵攻擊的步驟主要可以簡述成以下幾點：

1. 由外部對內部網路進行掃瞄(E1)
2. 藉由掃瞄所發現之弱點進行攻擊(E2)
3. 取得系統權限後，從網路上下載進一步的攻擊工具(E3)
4. 跟 C&C 伺服器連線，回報以及聽取命令(E4)
5. 對外進行掃瞄以及攻擊(E5)

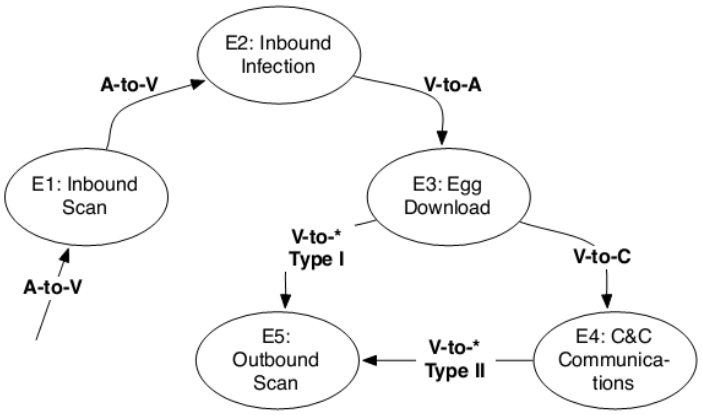

圖 1 攻擊步驟意示圖

殭屍網路為了避免被資訊安全人員以及執法單位追查到網路控制者的所在，控制者往往會根據跳板以及 C&C 伺服器進行指令的發佈，並將 C&C 伺服器及跳板散佈在世界各地，以增加追查的難度。在進行攻擊時，現在的殭屍網路會採用所謂的偵察者與侵入者模型，偵察者往往是新感染的電腦，攻擊者會以偵察者對受感染電腦所在網段進行大量掃描，並進行暴力破解登入的攻擊，其後再以侵入者對鎖定的目標進行攻擊與登入，用以規避傳統的入侵偵測系統。

Gu 等人(2007)以 Snort 為基礎，建立一個相關警告的聚合機制，BotHunter 能夠從許多的入侵警告中根據時間、來源 IP 位址以及警告種類來歸結出受到攻擊的種類，用以減少 Snort 過多警告的問題。後續研究 BotMiner，Gu 與 Perdisci(2008)，重點在於攻擊者連線的規律性，並取得惡意程式連線在網路流量觀察時所表現出來的特徵，進行進一步的深度檢視，以提高入侵偵測系統的效率與準確度。

除了以上所提到的方法，尚有針對 IRC 連線內容進行監聽與探測的 Gu 與 Porras、Stoll、Lee(2008)的 BotProbe、針對特定連線通訊協定進行內容監測，以對惡意程式可

能傳輸的可能相關進行過濾的 Gu 與 Lee(2008)的 BotSniffer，也有 Choi 等人(2007)針對群組 DNS 查詢請求進行連線規律性整理的殭屍網路偵測演算法，藉此來找到攻擊者的入侵跡象，以便能進行警告與防禦。

為了能夠規避此類防禦機制，殭屍網路發展出新攻擊手法，新方法採用聯合攻擊策略，也就是本研究所說的偵察者與侵入者攻擊策略，藉由使用價值較低的殭屍電腦進行廣泛而且顯眼的掃瞄與攻擊，在以較具價值的另一台殭屍電腦進行正常登入與進一步的攻擊，相關的技巧已經廣泛的被使用而且被觀察到了，本研究即欲解決此類問題，以應對針對此類弱點進行攻擊的攻擊技巧。

參、 系統架構

傳統的防禦與偵測方法對於防範偵察者與侵入者的聯合攻擊部份付之闕如，故本系統希望能夠彌補此部份之缺失。為此，本研究將需要收集網路上的流量，了解網路上的動態及活動，並同時取得主機內部資源調動及指令發佈之記錄，建立起惡意使用模式之模型，以之為偵測異常行為的根據。

系統將從網路監測系統以及主機本身記錄中進行相關的資料收集，再對網路流量進行檢測後，與主機工作日誌進行交叉比對，觀察網路行為，以隱藏式馬可夫鏈判斷其行為的合法性，以偵測偵察者與侵入者聯合攻擊。

各項目之元件介紹如下：

1. Network 資料收集模組：從網路骨幹進行側錄收集到的資料，以 Cisco 所制定之 Netflow 格式呈現，記錄區域網路內機器與區域網路外之機器之連線，並能顯示連線資料流大小與封包數，以供分析。
2. 系統監測資訊模組：從區域網路內主機之系統記錄截取相關資料，以取得主機內部接收或是拒絕連線之記錄，以及系統本身服務各種資源(記憶體、硬碟空間、連接埠)之開啟與關閉，與資料之傳輸狀況。
3. 網路資料截取模組：當受到攻擊時之網路流量資料截取，藉以分析判斷惡意程式正在執行之行為。
4. 資料聚合模組：收集來自網路與系統之記錄檔案，對其記錄進行關聯，進行時間相

依性之整合，過濾雜訊並且進行資料正規化。

5. 狀態判定模組：根據經過聚合與歸納之網路與系統記錄檔進行相對應執行狀態之認定與整合，以利 Detection Module 進行判斷。
6. 偵測模組：根據回傳之狀態與其記錄檔進行相對應機率之計算，並與已經過調整形成之隱藏式馬可夫鏈模型進行異同判定，來判定此次連線是否為惡意攻擊，並根據連線之惡意與否進行相對應的報告產生。

隱藏式馬可夫鏈模型是由一個可觀察之觀察序列與無法被觀察之狀態序列所構成。藉由整理狀態序列裡狀態所對應的觀察特徵，計算狀態所對應觀察特徵時，其發散的機率，

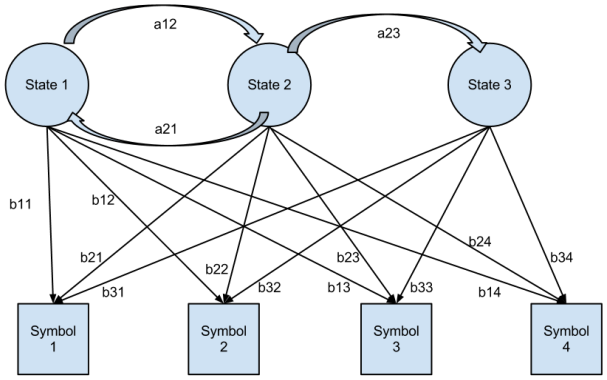

圖 2 隱藏式馬可夫鏈：隱藏狀態與觀察狀態

得知所為的觀察發散機率。於觀察時我們會發現到一連串由觀察特徵所構成的觀察序列，藉由這些觀察序列，我們可以根據系統現在所在的狀況推斷出狀態序列內相對應狀態轉移之機率，以此建立模型，作為偵測時之判斷依據。

以圖 2 為例，狀態序列內有 State 1~3 之狀況，根據不同的狀態，觀察特徵值 Symbol 1~4 所對應的發散機率也不同，在單一狀態下，其觀察特徵發散機率之總合應為 1：

$$\sum_{i=1}^{n} b_{1i} = 1,\ n=4(1)$$

藉由訂定義好的模型，我們可以根據所觀察到的觀察特徵值出現的機率與目前的狀態的轉移機率得知攻擊者的意圖，以及所受攻擊的階段辨別。

本研究以此特性，根據從網路及主機端所收集到的惡意使用者的攻擊手法，再將惡意使用者所執行之惡意使用步驟以隱藏式馬可夫鏈模型定義出根據其行為出現機率的惡意使用之模型，再根據此模型進行檢測，如果是正常使用者所做出的正常使用行為，使用者對於主機的操作記錄會於不同的狀態中顯示出異於以惡意使用者行為建構之模型中對應狀態之機率，本研究使用檢測的各個狀態根據其對於惡意攻擊行為成立之機率來判斷受測之使用者行為是否為惡意攻擊行為。

偵測聯合攻擊之困難處在於如何將前述偵察者之網段掃瞄以及暴力密碼攻擊等動作與侵入者之一次性正常登入進行整合與聯結，在長期的觀察當中，本研究發現偵察者於暴力密碼攻擊成功後，會立即的登出受害系統，之後在一定時間長度 T 內，侵入者會以偵察者發現的帳號與密碼組合進行第一次登入即成功、不會觸發系統警告的正常登入。

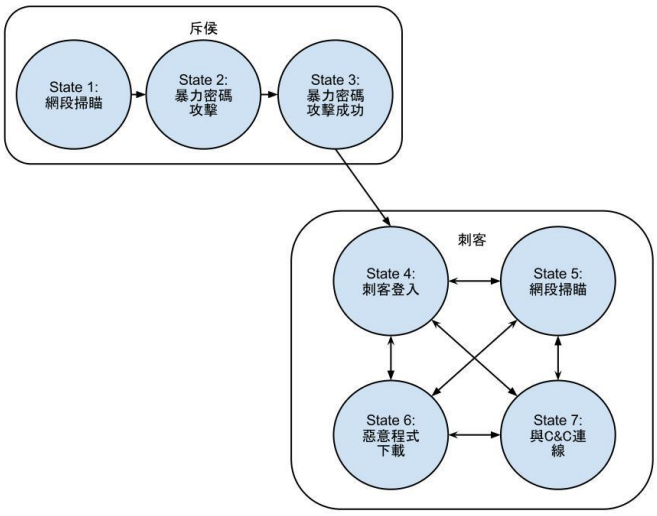

圖 3 偵察者與侵入者攻擊狀態圖

為克服此類攻擊，本研究以 Netflow 資料對網路連線進行監測，一旦發現來自外部的掃瞄後，即回報系統，該主機在本研究所建立之偵測模型即被記錄，且進入偵測系統的 State 1。

在發現網段受到掃瞄後，本研究觀察到隨之而來的，常常是針對登入系統的暴力密碼攻擊，根據我們所設計的系統記錄處理程式，將來自各個主機的嘗試時間、次數、嘗試時間區間分別記錄下來，根據嘗試的時間與次數進行評斷來訪的主機是否是在進行暴力密碼

攻擊。此時系統會將偵測狀態由 State 1 調整為 State 2，開始注意帳號登入狀況，一但帳號登入後，偵察者往往會立即登出，此時偵測狀態轉為 State 3。

系統受到暴力密碼攻擊後，任何於 T 時間內於該系統登入之帳號皆會受到注意，並將之與系統內部建立之名單之登入資訊記錄進行相似性比對，一但使用者登入相關資訊與上次一次登入資訊間的異變超出容許範圍，系統即會對該登入使用者進行密切的觀察，此時該主機於本研究所建立之偵測系統內之狀況進入 State 4。

當主機內於偵測系統狀態為 State 4 後，偵測系統將同時對該使用者於系統內之行為、該主機連線位置進行記錄，以及傳輸資料進行截取，一旦使用者開始進行可能會對系統或是所在網段造成傷害、或是攻擊之行為，像是進行網段掃描(State 5)、惡意程式下載(State 6)，甚或利用弱點攻擊程式進行攻擊(State 7)時，即根據操作行為所累積評斷的評估值進行威脅計算，一但超過範圍值，即發出警訊，並將聯合攻擊模式中的偵察者與侵入者主機的來源位置、攻擊手法、嘗試次數以及下載資料回報與管理者，進行整合，以供管理者進行判斷。

藉由統計惡意程式在進行攻擊時，對於隱藏狀態間的轉移記錄，以及隱藏狀態與其相對應觀察特徵的出現分佈，我們可以推估出偵察者與侵入者聯合攻擊之狀態轉移機率以及對應的觀察特徵發散機率，再將相關的模型與我們實際收集到的資料進行調整後，當模型收斂到某一階段，我們可以得出一個聯合攻擊偵測用的隱藏式馬可夫鏈模型，以此一模型對系統的使用過程中進行推估，一但使用者有可能是為惡意的使用者，則即早通知系統管理員，協助注意。

肆、結論與未來研究方向

本研究試圖以隱藏式馬可夫鏈協助偵測近來觀察到的偵察者與侵入者攻擊現象，在找出攻擊者進行攻擊時，所被偵測到的特徵現象其組合背後所代表的意義，以求能對此一聯合攻擊型態在早期發動時即加以偵測，並提出警告。未來本研究將朝向針對偵察者與侵入者間的關聯強度進行改進，對使用者登入資訊建立資料群組，以距離演算法對相關資訊進行計算，以求能更精準的判定使用者異常登入狀況，以此降低系統誤判率。

參考文獻

1. Castells, M. , “The Rise of the Network Society: The Information Age: Economy, Society, and Culture Volume I, 2nd Edition with a New Preface” , Blackwell, 2009,
2. Shadowserver, “Botnets”, Shadowserver, 2005, (Available from: http://www.shadowserver.org/wiki/pmwiki.php/Information/Botnets)
3. The H-security, “Botnet attacks pizza delivery service”, The H-security, 2011, (Available from: http://www.h-online.com/security/news/item/Botnet-attacks-pizza-delivery-service-1330816.html)
4. Thompson, M., “Mariposa Botnet Analysis”, Defence Intelligence, 2010 (Available from: http://defintel.com/docs/Mariposa_Analysis.pdf)
5. Newswire, P. ,” *Panda Security and Defence Intelligence Coordinate Massive Botnet Shutdown with International Law Enforcement.*”, Newswire, 2011 (Available from: http://www.prnewswire.com/news-releases/panda-security-and-defence-intelligence-coordinate-massive-botnet-shutdown-with-international-law-enforcement-86189032.html)
6. Li,Z, Liao,Q., Striegel, A., “Botnet Economics: Uncertainty Matters” In Managing Information Risk and the Economics of Security (2009), pp. 245-267
7. Krebs,.B., “Rent-a-Bot Networks Tied to TDSS Botnet“, KerbsonSecurity, 2011(Available from: http://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/)
8. Gu, G., Porras, P., Yegneswaran,V., Fong,M., and Lee,W., “BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation.” *In Proceedings of the 16th USENIX Security Symposium(Security07)*, 2007.
9. Gu, G., Perdisci, R., Zhang, J., and Lee, W., “BotMiner: clustering analysis of network traffic for protocol- and structure-independent botnet detection.” , *In Proceedings of the 17th USENIX Security Symposium (Security08)*, 2008.
10. Ramachandran, A., Seetharaman, S. ,Feamster, N., and Vazirani, V., “Fast monitoring of traffic subpopulations.” ,*In Proceedings of the 8th ACM SIGCOMM conference on Internet measurement*, 2008, pp. 257-270.
11. Gu,G., Yegneswaran,V., Porras,P., Stoll,J.,and Lee,W., “Active Botnet Probing to Identify Obscure Command and Control Channels.” *In Proceedings of the 16th USENIX Security Symposium.(Security07)*, 2007.
12. Gu,G., Zhang, J., Lee,W., “BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic.”, I*n Proceedings of the Annual Network and Distributed System Security Symposium(NDSS'08),* 2008.
13. Choi,H., Lee,H., Lee,H.,Kim,H., “Botnet Detection by Monitoring Group Activities in DNS Traffic”, *In Proceedings of the 7th IEEE International*

Conference on. 2007.

Detecting Botnet-based Joint Attacks

Chia Mei Chen
Department of Information Management National Sun Yat-sen University
cchen@mail.nsysu.edu.tw
Han Wei Hsiao
Department of Information Management Nation University of Kaohsiung
hanwei@nuk.edu.tw
Chung-Nan Lee
Department of Computer Science and Engineering National Sun Yat-sen University
cnlee@cse.nsysu.edu.tw
Chung-Huang Yang
Graduate Institute of Information and Computer Education National Kaohsiung Normal University
chyang@nknucc.nknu.edu.tw
Peng Yu Yang
Department of Information Management National Sun Yat-sen University
M994020007@student.nsysu.edu.tw

Abstract

We present a new detection model include monitoring network perimeter and hosts logs to counter the new method of attacking involve different hosts source during an attacking sequence. The new attacking sequence we called "Scout and Intruder" involve two separate hosts. The scout will scan and evaluate the target area to find the possible victims and their vulnerability, and the intruder launch the precision strike with login activities looked as same as authorized users. By launching the scout and assassin attack, the attacker could access the system without being detected by the network and system intrusion detection system. In order to detect the Scout and intruder attack, we correlate the netflow connection records, the system logs and network data dump, by finding the states of the attack and the corresponding features we create the detection model using the Hidden Markov Chain. With the model we created, we could find the potential Scout and the Intruder attack in the initial state, which gives the network/system administrator more response time to stop the attack from the attackers.

Keywords: Botnet, Hidden Markov Chain, Intrusion Detection System