TLP:WHITE

後門程式 More_eggs 與
無檔案載入程式 PSLoramyra
分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 01 月

一、事件簡介

1. 2024/4 某資安公司研究人員發現偽裝成履歷表的惡意軟體 More_eggs，在針對人事部人員進行網路釣魚攻擊。
2. 2024/11 趨勢科技的客戶在人事部門招募人才時，因為人員不慎下載假的履歷表，執行一個惡意.LNK 檔，最後造成電腦感染 more_eggs 惡意程式。
   (1) 駭客假扮成應徵者「John Cboins」，而且寄出一封魚叉式網路釣魚信件給該公司的一名高階主管。
   (2) 在信件中無任何附件或連結，推測此作法在企圖取得收件者的信任。
   (3) 接著該公司的人員使用瀏覽器於求職者個人網站下載假的履歷表「John Cboins.zip」。
   (4) 該網站有內建 CAPTCHA 人機驗證測試，讓網頁無可疑的地方，該公司人員不小心的話很容易受騙上當。
3. 因為偽裝成履歷表的 More_eggs 攻擊手法從 2024/4 被發現至今仍持續中，在學網學校徵聘人才的工作是常態性業務。為了有效預防遭受 More_eggs 的攻擊，故進行該惡意軟體的分析。
4. 2024/11 無檔案載入程式 PSLoramyra 產生，它被用來散播遠端存取木馬 Quasar RAT。
   (1) 它採用複雜的規避方法來繞過偵測，讓受害者無法知道它的存在。
   (2) 若感染它，駭客能遠端操控電腦與竊取資料，故分析該惡意軟體的攻擊行為將可有效預防與偵測它。

二、 後門程式 More_eggs

1. more_eggs 是一個 JScript 後門程式，為 Golden Chickens 工具套件之一。

它被駭客組織(例如:FIN6 與 Cobalt Group)使用來攻擊金融業與零售業，而且它會從 C2 Server 下載其他惡意程式來執行。它會在受感染的電腦上秘密地執行著，因此在電腦上沒有明顯的特徵。

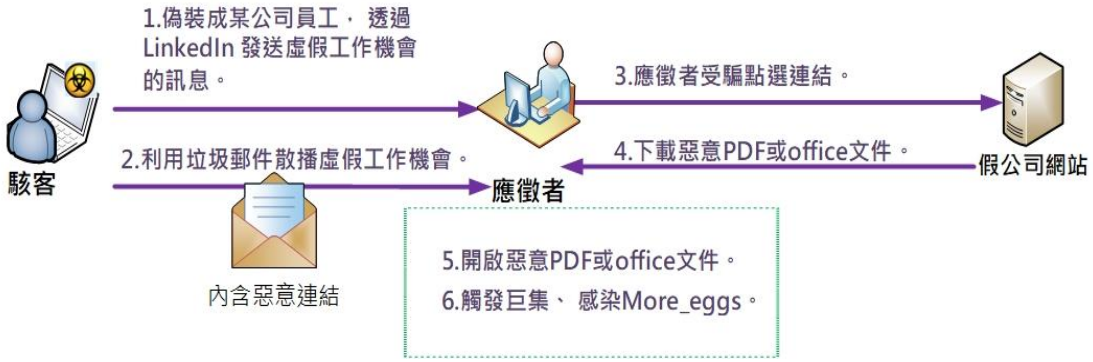
2. 它的散播方式如下:

(1) 它通常利用垃圾郵件進行散播。例如:使用電子郵件附件、惡意的線上廣告、惡意的軟體破解檔。

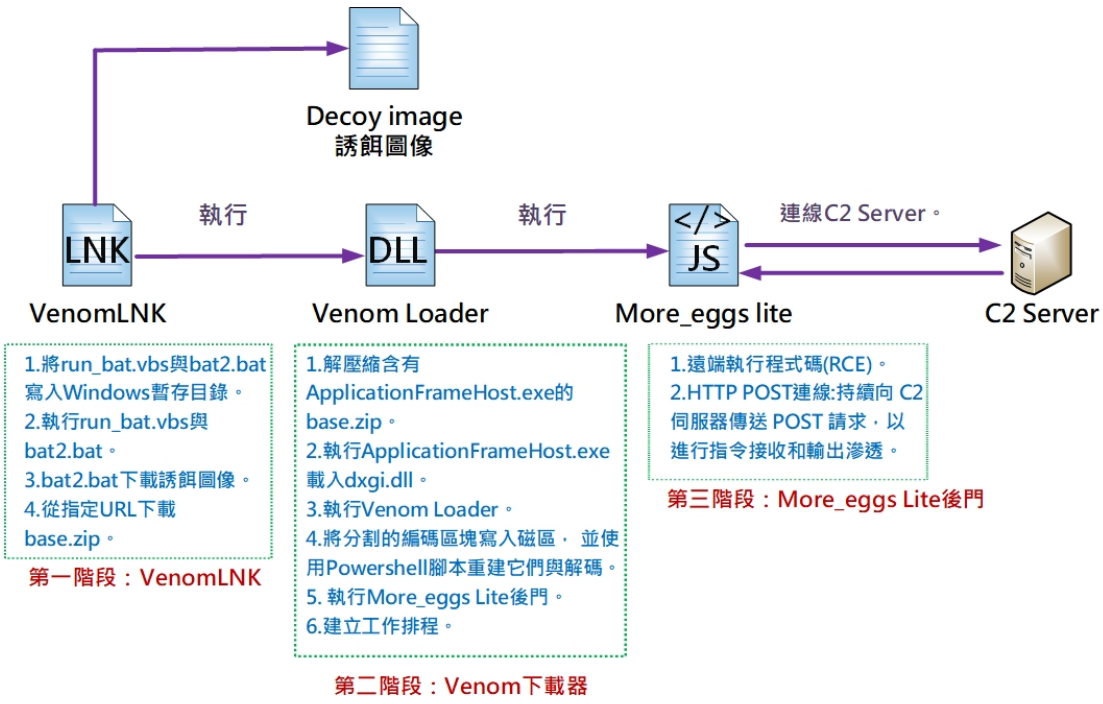
(2) 以前它的攻擊目標為應徵者，試圖誘騙應徵者開啟惡意附件或點選(下載)其他文件的網站連結，現在則以誘騙負責招收人才的人事部人員為對象。

3. 它的攻擊可能造成的損害有密碼外洩、受害者的電腦被添加到殭屍網路、造成資料遺失、發生隱私問題等。

4. 傳統感染 more_eggs 的方式如下圖所示，首先駭客偽裝成某公司員工透過 Linkedln 發送假的工作機會訊息，接著利用垃圾郵件散播虛假工作機會。應徵者收到垃圾郵件後受騙點選信件中的惡意連結，之後連上甲公司網站下載惡意 PDF 或 office 文件。最後，應徵者會開啟檔案、觸發巨集，感染了 More_eggs。



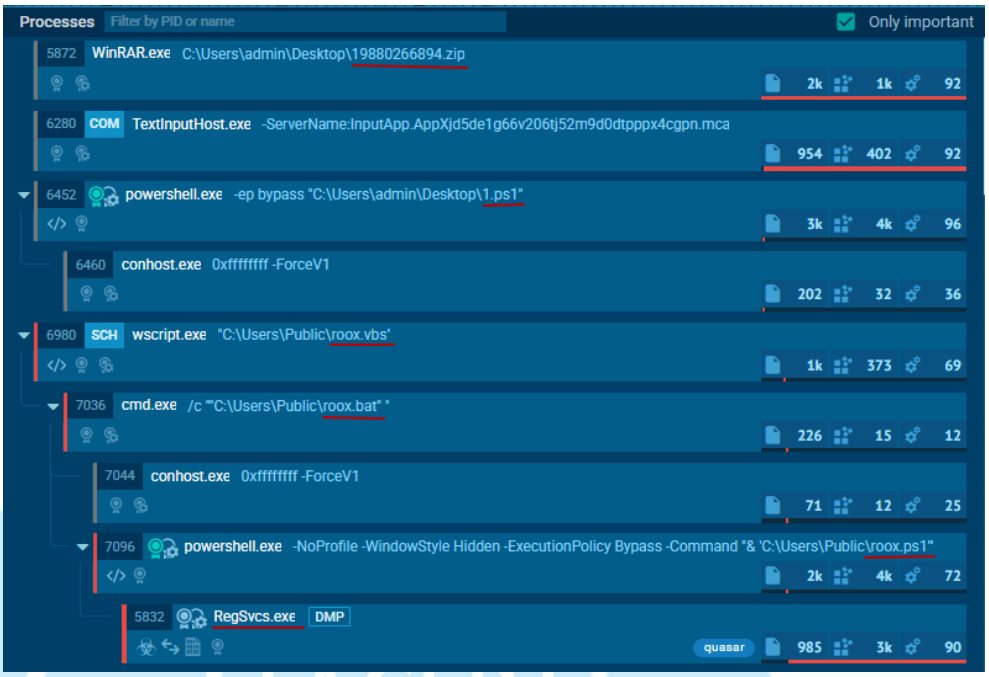
5. 新型感染 more_eggs 的方式如下圖所示，2024/12 網路安全公司在 08~ 10 月期間觀察到 More_eggs 透過 Venom Loader 散播。它使用加密貨幣交易為誘餌來提供 Venom Loader，隨後載入 More_eggs Lite。

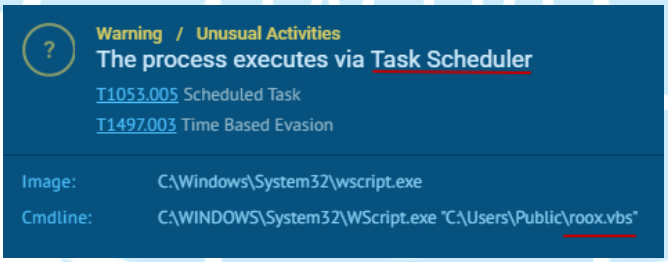


三、 無檔案載入程式 PSLoramyra

1. PSLoramyra 是一種無檔案的惡意軟體載入程式，它利用 PowerShell、VBS 和 BAT 腳本直接在記憶體中注入和執行惡意 payload，來逃避偵測。它會在感染的電腦上秘密的執行著，因此在受害者不容易發現它的存在。
2. 它的散播方式為利用受感染的電子郵件的附件、惡意網路廣告、惡意的軟體「破解」檔案進行散播。
3. 它可能造成的損害有密碼和銀行資訊可能被盜、身分被盜竊、受害者的電腦被添加到殭屍網路中。
4. PSLoramyra 樣本檢測
   (1) 在 ANYRUN 沙箱下檢測 PSLoramyra 樣本 19880266894.zip (MD5:ed317f14874222307a0d5107eabf00af)。
   (2) 該樣本執行後會先解壓縮，接著依序執行下列檔案。執行初始腳本 1.ps1 會產生下面三個檔案(roox.vbs、roox.bat 與 roox.ps1)，接著執行

roox.vbs，它會啟動 roox.bat。之後 roox.bat 執行後呼叫 roox.ps1 來執行，roox.ps1 執行後會呼叫 RegSvcs.exe 來執行。Roox.vbs 因為有設定工作排程，會一直啟動重新執行。

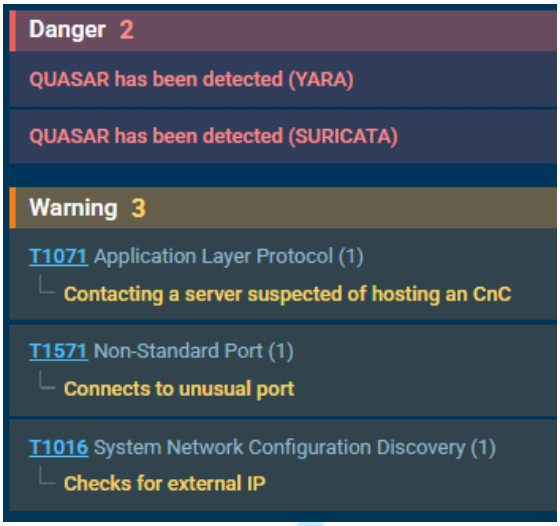


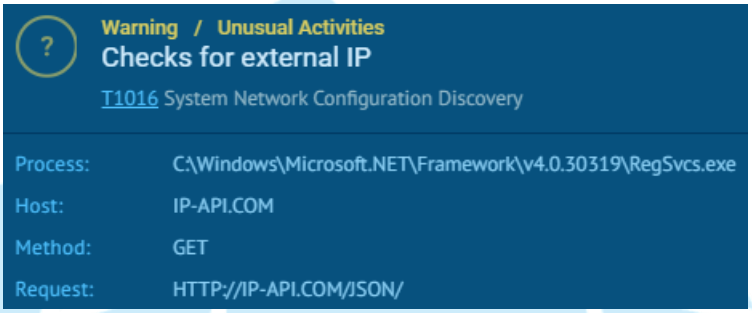


(3) 當 RegSvcs.exe 執行時，會執行 QUASAR 與連線 C2 Server (IP:3.145.156.44)，而且連線時使用異常 Port(Port:4782)，也會連線檢查外部網址/IP (HTTP://IP-API[.]COM/JSON/)。

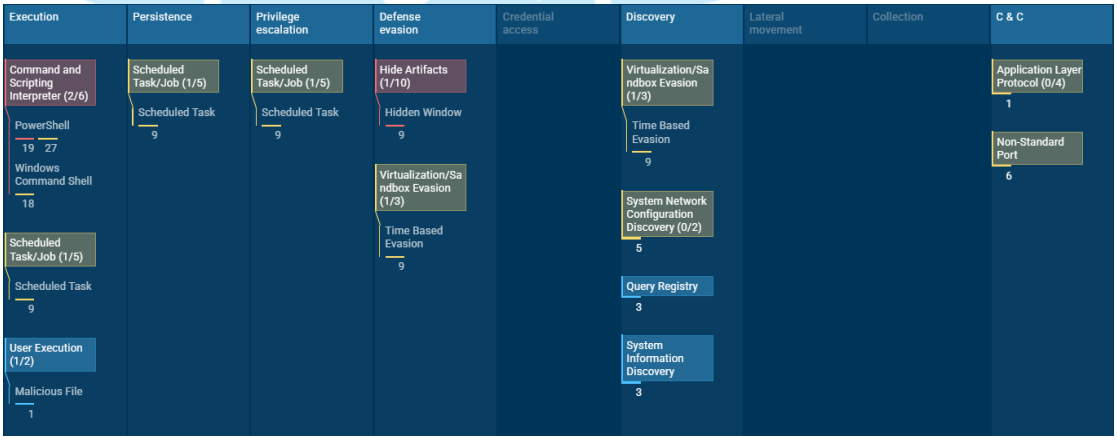
IP	Domain	Virustotal (IP;Domain)	AbuseIPDB (舉報次數/最後舉報日期)
208.95.112.1 (美國)	ip-api.com	1/94; 0/94	73 次 /2024-12-31
3.145.156.44 (美國)	ronymahmoud.casacam.net	10/94; 15/94	-

Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN
TCP		5832	RegSvcs.exe		208.95.112.1	80	ip-api.com	TUT-AS
TCP		5832	RegSvcs.exe		3.145.156.44	4782	ronymahmoud.casacam.net	AMAZON-02





(4) 以 MITRE ATT&CK Matrix 分析 PSLoramyra，發現該樣本所運用技術橫跨 Execution、Persistence 、 Privilege escalation、Defense evasion、Discovery 與 C&C 等 6 個階段，其中包含執行腳本、建立工作排程與連線 C&C Server。



5. PSLoramyra 之規避技巧

它採用一套複雜的規避技巧來繞過偵測

(1) 無檔案執行: 將惡意程式碼直接注入記憶體，而不將檔案寫入磁碟來逃避檢測。

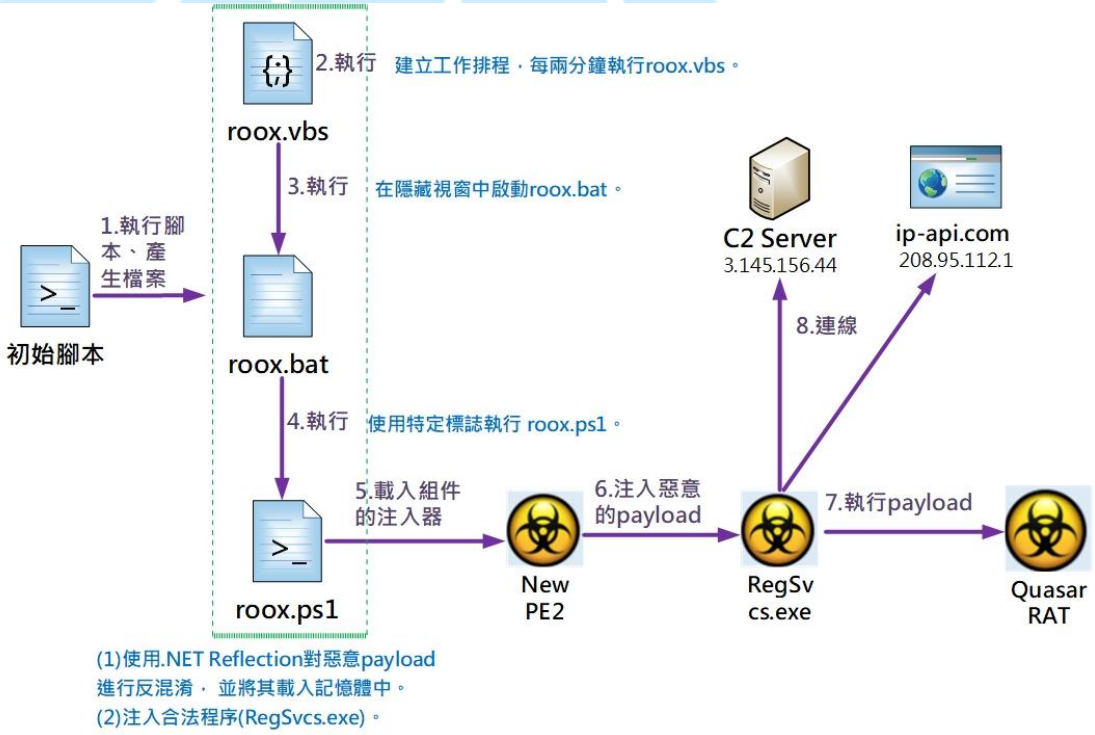
(2) 採用混淆手法: 使用帶分隔符號的十六進位編碼，使靜態分析變得複雜。刪除 # 符號以清除混淆的方法名稱，來阻礙分析工作。

(3) 隱形程式的注入: 將 payload 注入合法的 Windows 程式 RegSvcs.exe，以隱藏在正常系統中 PSLoramyra 的執行。

(4) 隱藏執行行為: 在隱藏視窗中執行腳本，防止使用者察覺。

(5) 透過合法服務持續存在於電腦中: 使用如 GoogleUpdate 之類的名稱登記工作排程，讓它可以每兩分鐘重新執行腳本。

6. PSLoramyra 感染鏈如下圖所示，起初由執行初始腳本產生檔案後，陸續建立工作排程來執行 roox.vbs、啟動 roox.bat、執行 roox.ps1、注入惡意 payload，最後執行 payload 與連線 C2 Server。



四、 總結與建議

1. 經由分析本案兩個惡意程式 More_eggs Lite 與 PSLoramyra，發現兩者在執行後於受害者電腦內無任何明顯特徵，但是可由兩者皆會連線 C2

Server 的行為來判斷是否感染惡意程式。

2. 比較兩者的差異性，可得知 PSLoramyra 使用較多的規避偵測的技巧。
   (1) More_eggs Lite 利用 JS 後門執行遠端程式碼，與 PSLoramyra 使用 PowerShell 和 BAT 腳本來執行不同。
   (2) PSLoramyra 會將 payload 注入合法的系統程序中（RegSvcs.exe），以隱藏其惡意行為。
   (3) PSLoramyra 在記憶體中執行，無需建立檔案，因此增強隱蔽性和規避偵測。
   (4) PSLoramyra 使用系統特定的環境變數對 payload 進行編碼，來造成混淆。
3. 在處理兩個惡意程式的攻擊事件方面，可採用下面幾個面向來偵測與防範。
   (1) 行為分析
      (a) 腳本執行監控:可透過辨別 roox.vbs、roox.bat 和 roox.ps1 等腳本的建立和執行來判斷。
      (b) 程序注入檢測: 檢查是否有合法程序(如:RegSvcs.exe)被注入。
      (c) 稽核工作排程:仔細檢查是否有高頻率觸發或可疑名稱的工作排程在受害電腦內。
   (2) 網路流量監控
      檢測 C2 server 的連線與異常流量的檢測。
   (3) 腳本和檔案監控
      (a) 檔案系統監控:檢查公用目錄中是否有檔案建立，以及是否存在已知的惡意腳本。
      (b) 腳本內容分析:分析 PowerShell、VBS 和 BAT 腳本的內容來尋找混淆模式、十六進位編碼和可疑命令。
      (c) 將 PowerShell 限制為僅執行已簽署的腳本，來防止執行未經授

權或惡意的腳本。

(d) 採用腳本白名單，僅允許核准的腳本在環境中執行。

(4) 端點保護

採用 EDR 應該能夠偵測到記憶體內的執行、程序注入和異常腳本等行為。

(5) 審核持久化機制

(a) 工作排程安全性：定期審核工作排程是否有未經授權的工作，尤其是名稱模仿的工作排程。

(b) 註冊表監控：查看開機自動執行的程序是否有未經授權的修改。

(6) 教育使用者和建立資安意識

(a) 預防網路釣魚攻擊的訓練：培訓使用者識別網路釣魚的攻擊手法，養成使用者不隨意開啟不明來源的檔案或不點選不明連結的習慣。

(b) 資安意識計劃：實施定期的資安意識計劃，讓使用者了解不斷變化的資安威脅和社會工程的攻擊手法。

參考資料

1. **駭客也在找工作？ 趨勢科技 MDR 識破假履歷，緊急攔截鎖定人資部門的 More_eggs 後門威脅！**
https://www.trendmicro.com/zh_tw/research/24/i/mdr-in-action--preventing-the-moreeggs-backdoor-from-hatching--.html
2. **More_eggs Malware Disguised as Resumes Targets Recruiters in Phishing Attack**
https://thehackernews.com/2024/06/moreeggs-malware-disguised-as-resumes.html
3. **More_eggs MaaS Expands Operations with RevC2 Backdoor and Venom Loader**
https://thehackernews.com/2024/12/moreeggs-maas-expands-operations-with.ht

ml

4. **PSLoramyra: Technical Analysis of Fileless Malware Loader**
   https://any.run/cybersecurity-blog/psloramyra-malware-technical-analysis/
5. **RevC2, More_eggs Lite & PSLoramyra: Insights into Advanced Fileless Malware**
   https://www.secureblink.com/threat-research/rev-c2-more-eggs-lite-and-ps-loramyra-insights-into-advanced-fileless-malware
6. **How to remove More_eggs malware from your computer**
   https://www.pcrisk.com/removal-guides/14567-moreeggs-malware
7. **How to remove PSLoramyra loader-type malware from the operating system**
   https://www.pcrisk.com/removal-guides/31634-psloramyra-malware
8. **ANYRUN 檢測 PSLoramyra 樣本 19880266894.zip**
   https://app.any.run/tasks/24dbdd79-5ff1-4050-8ac3-9edb348ff923