TLP:WHITE

駭客組織 Silver Fox 之攻擊行為分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2025 年 02 月

一、事件簡介

1. 2024/08 FortiGuard Lab 發現 ValleyRAT 專門針對中文使用者攻擊。
2. 2025/01 Intezer Labs 發現駭客組織 Silver Fox 使用惡意程式 PNGPlug、ValleyRAT，鎖定攻擊範圍為臺灣、香港、中國。
3. 2025/02 資安公司 Morphisec 公布駭客組織 Silver Fox 一改過去攻擊方式，假借提供瀏覽器 Chrome 安裝程式、簡訊服務等名義來散播 ValleyRAT。
4. 有鑑於 Silver Fox 的攻擊活動頻繁，加上鎖定臺灣為其攻擊對象，故分析該組織的攻擊行為是值得探討的議題。

二、 駭客組織 Silver Fox

1. Silver Fox（又稱為 Silver Fox APT）是一個以中國為基地的高級持續性威脅（APT）組織，專門針對講中文的個人和組織進行網路間諜活動。自 2022 年以來，該組織一直很活躍，它利用電子郵件、釣魚網站、即時通訊軟體等多種管道散播木馬，而且瞄準各公司的財務、會計、銷售等部門人員或主管進行攻擊。
2. 該組織所採用的策略有兩種如下。
   (1) 網路釣魚技術：使用木馬檔案和 SEO 優化的網路釣魚網站。它使用 SEO（搜尋引擎優化）來確保釣魚網站在中文搜尋引擎結果中排名靠前。透過 SEO 來利用惡意廣告和多個電子郵件的網路釣魚活動來散播遠端管理木馬，例如:ValleyRAT。
   (2) 間諜工具：部署 ValleyRAT 和 Gh0st RAT 等惡意軟體來監視使用者活動、傳送外掛程式並可能安裝其他有效 payload。
3. ValleyRAT 是由駭客組織 Silver Fox 所編寫的木馬程式，於 2023 年首次被發現。它是一個功能強大的後門程式，可遠端操控被駭主機，例如:

螢幕擷取、 鍵盤側錄、執行檔案、植入惡意外掛程式等。它的執行階段包括初始執行、部署混淆的 shellcode ，以及從 C2 伺服器取得其他惡意元件的載入器模組。

4. ValleyRAT 是一種複雜的多階段惡意軟體，採用了先進的技術如下：

(1) 執行 Shellcode:直接在記憶體中執行元件，以減少檔案佔用空間與利於逃避偵查。

(2) 混淆和權限提升:隱藏攻擊行動並獲得提升的存取權限。

(3) 持久性機制:利用工作排程和登錄檔修改來維持對受感染系統的控制。

三、 駭客組織 Silver Fox 之攻擊工具與攻擊鏈

1. 有關駭客組織 Silver Fox 攻擊常用工具在 2024/6 Knownsec 404 Advanced Threat Intelligence Team 的追蹤 Silver Fox 攻擊過程中，發現相關的攻擊工具如下。

(1) Winos 木馬

它是 Silver Fox 針對稅務、財務人員的攻擊中多次使用的 payload。攻擊者將 Winos 偽裝成 360 Chrome 瀏覽器，但它的程式圖示和屬性直接洩漏它是假的程式。它採用 VMP（Virtual Machine Protect）進行程式碼保護，目的是阻止它被資安人員進行分析。

(2) UpdateDll 下載器

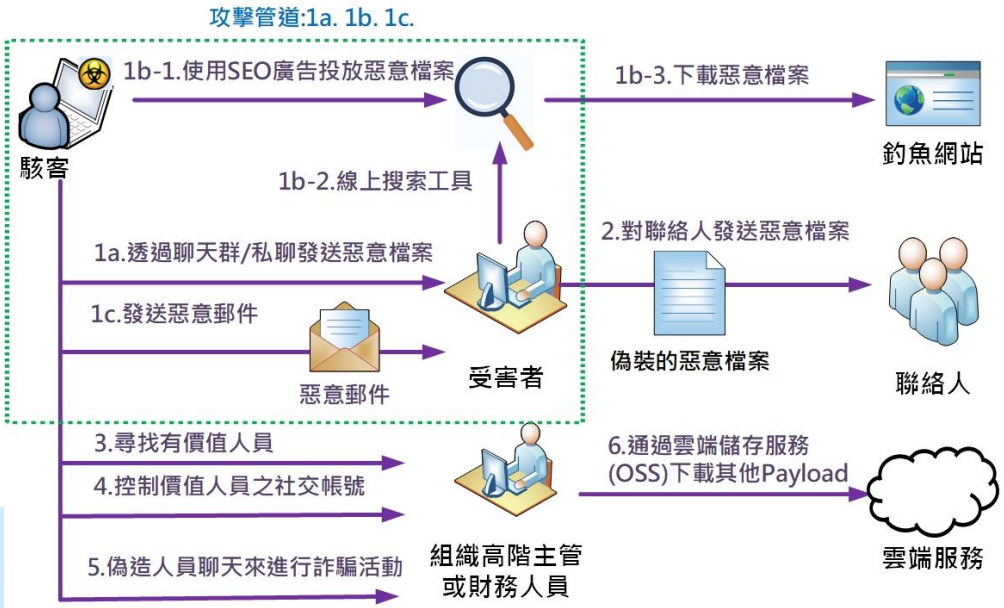
主要功能在從指定位址下載 DLL 並執行。

(3) powershell 混淆工具 Out-EncodedSpecialCharOnlyCommand

它是將 PowerShell 腳本程式碼轉換為純符號程式碼的工具，可被攻擊者用來增強惡意 payload 的混淆效果。

2. 在駭客組織 Silver Fox 常採用之攻擊鏈方面，下圖為 2023 年 Silver Fox

常採用的攻擊方式示意圖。攻擊管道可分為兩種: (1.)以聊天軟體散播惡意檔案為主要途徑。(2.)以郵件或 SEO 廣告偽造的釣魚網站來傳播惡意檔案。



圖片來源: TACERT 整理、資料來源:https://www.secrss.com/articles/60688

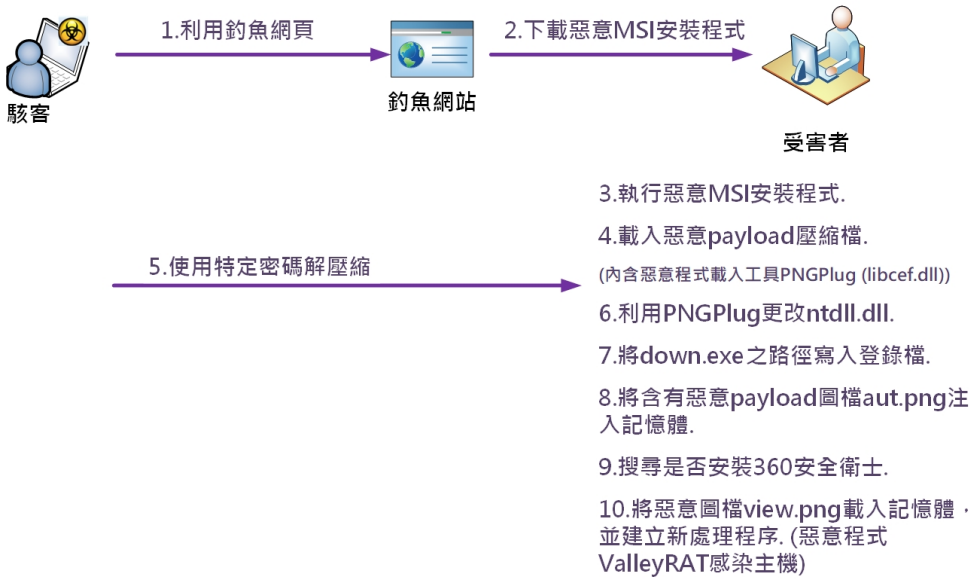
3. Silver Fox 散播 ValleyRAT 之新攻擊方式一如下，2025/01 Intezer Labs 發現針對香港、台灣和中國大陸等地區的攻擊。這些攻擊利用多層載入程式 PNGPlug 來傳送 ValleyRAT 的有效 payload。它使用釣魚網頁，鼓勵受害者下載偽裝成合法軟體的惡意 MSI（Microsoft Installer）安裝程式。執行後，安裝程式將執行兩個任務：(1)安裝合法的應用程式來維持程序合法性的假象。(2)擷取包含惡意軟體 payload 的加密檔案。這個新攻擊方式使用之程式如下。

   (1) libcef.dll:為載入程式 PNGPlug，採用填充設計，將檔案大小增加到 220MB，因為許多安全工具會跳過對大檔案的分析，有助於逃避偵測。

   (2) down.exe:是用於遮掩攻擊活動的合法應用程式。

   (3) aut.png 與 view.png:為偽裝成 PNG 圖像的文件，其中包含編碼的惡意 payload。

4. Silver Fox 散播 ValleyRAT 之新攻擊鏈一如下圖所示，駭客利用釣魚網頁讓受害者從釣魚網站下載惡意的 MSI 安裝程式，而在受害者執行安裝程式後會載入惡意 payload 壓縮檔。之後修改 dll 檔案與登錄檔，並將惡意 payload 注入記憶體後，讓主機感染 ValleyRAT。



圖片來源: TACERT 整理、資料來源:https://www.ithome.com.tw/news/167099

5. Silver Fox 散播 ValleyRAT 之新攻擊方式二如下，2025/2 Morphisec 發現 Silver Fox 近期改變了攻擊手法，利用多階段攻擊鏈，並透過假冒瀏覽器安裝程式的下載網站和簡訊服務網站，搭配使用抖音的執行檔，在受害者主機的記憶體中載入惡意 DLL，最終使主機感染 ValleyRAT。在這些攻擊中，Silver Fox 使用了以下攻擊程式：

(1) sscronet.dll：這個動態連結庫（DLL）檔案在記憶體中載入，協助執行後續的 douyin.exe。

(2) douyin.exe：這是中國版抖音的執行檔，被用來下載其他惡意程式。攻擊者特別選用抖音這類常見的中文應用程式作為下載軟體，以降低使用者的戒心。

(3) tier0.dll：這個 DLL 檔案在記憶體中載入，協助執行 ValleyRAT。

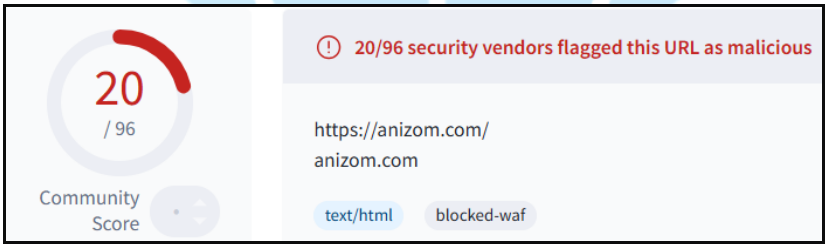
(4) mpclient.dat：這是一個加密的 Shell Code 檔案，最終被解密並執行

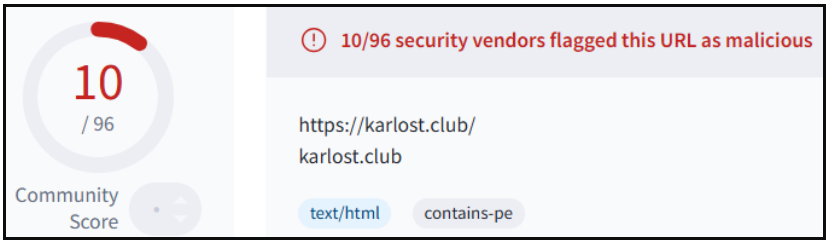
ValleyRAT。

6. Silver Fox 散播 ValleyRAT 之新攻擊鏈二如下圖所示，駭客誘騙受害者至惡意網站下載惡意的 Chrome 安裝程式 Setup.zip，解壓縮後執行安裝程式 Setup.exe。在提權至管理者權限後，下載 sscronet.dll 等三個工具，並且在記憶體內載入 sscronet.dll、執行 douyin.exe 與解密 mpclient.dat。最後，執行 ValleyRAT 讓受害主機感染它。

圖片來源: TACERT 整理、資料來源:https://www.ithome.com.tw/news/167254

駭客所用的兩個惡意網站 https[://]anizom[.]com 與 https[://]karlost[.]club 經 Virustotal 檢測其惡意比例分別為 20/96 與 10/96，皆為惡意網站。





四、 總結與建議

1. 經由分析 Silver Fox 散播 ValleyRAT 之攻擊鏈，發現最早期該組織的攻擊對象為中國，攻擊者通過當地聊天軟體或利用釣魚方式對許多公司進行攻擊。將惡意檔案偽裝為辦公室軟體、軟體工具安裝包、發票、財務或稅收等相關業務檔案，來誘騙受害者執行檔案。
2. 近期該組織散播 ValleyRAT 的管道偏向使用釣魚網站，提供下載安裝軟體來誘騙使用者，而且攻擊對象以中文使用者為主，範圍包含臺灣。
3. 由於受害者被誘騙至惡意網站下載惡意檔案後導致感染 ValleyRAT，故在防範建議方面有下列幾點提供參考。
   (1) 不從未知網站下載軟體安裝程式，建議優先從官網下載。
   (2) 對於他人寄送來之檔案，建議與寄送者確認後再打開。
   (3) 不隨意開啟不明來源附檔或瀏覽不明網站。
   (4) 建議實施嚴格的 DLL 載入政策，並監控異常的 DLL 載入行為。

參考資料

1. 銀狐獵影：深度揭示銀狐團夥技戰法
https://www.secrss.com/articles/60688
2. Unearthing New Infrastructure by Revisiting Past Threat Reports
https://hunt.io/blog/unearthing-new-infrastructure-by-revisiting-past-threat-reports
3. Analysis of the Suspected APT Attack Activities by "Silver Fox"
https://medium.com/@knownsec404team/analysis-of-the-suspected-apt-attack-activities-by-silver-fox-25781647da2b
4. A Deep Dive into a New ValleyRAT Campaign Targeting Chinese Speakers
https://www.fortinet.com/blog/threat-research/valleyrat-campaign-targeting-chinese-speakers
5. [原創]釣魚網頁散播銀狐木馬，遠控後門威脅終端安全
https://bbs.kanxue.com/thread-284691.htm

6. Threat Bulletin: Weaponized Software Targets Chinese-Speaking Organizations

https://intezer.com/blog/malware-analysis/weaponized-software-targets-chinese/

7. 惡意程式 PNGPlug、ValleyRAT 鎖定臺灣、香港、中國地區而來

https://www.ithome.com.tw/news/167099

8. Rat Race: ValleyRAT Malware Targets Organizations with New Delivery Techniques

https://www.morphisec.com/blog/rat-race-valleyrat-malware-china/

9. 駭客組織 Silver Fox 假借提供瀏覽器、簡訊服務名義，意圖散布惡意軟體 ValleyRAT

https://www.ithome.com.tw/news/167254