TLP:WHITE

載入程式 HijackLoader 之分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2024 年 05 月

一、事件簡介

1. 在 2023 年 7 月 HijackLoader 首次被發現，此後被用於針對各個行業組織（包括飯店業）的攻擊中。它能夠使用各種模組進行程式碼注入和執行，這是大多數載入器不具備的功能，其模組化設計是它受歡迎的關鍵因素之一。

2. **HijackLoader 對飯店攻擊之案例**

   攻擊者透過電子郵件與飯店聯繫以預訂房間，並以食物過敏為藉口寄送含有惡意壓縮檔的下載連結。這些連結通常指向信譽良好的雲端硬碟服務平台（例如:dropbox.com、drive.google.com 等）來提供檔案下載 。攻擊者也透過 Booking 與飯店聯繫，並使用非常類似的方式； 它們告知飯店應考慮的某些禁忌症狀，以避免所附醫療處方中描述的某些過敏問題。上述的行為皆在誘騙收信的工作人員下載包含其過敏資訊的檔案。一旦打開，該檔案就會啟動感染鏈，導致在受害者的裝置上安裝 HijackLoader。

3. HijackLoader（又稱 IDAT Loader）是一種載入器惡意軟體，具有強大的規避能力，可以繞過主流安全措施，可在受感染系統上散播不同類型惡意軟體。根據觀察，它散播了許多持久性惡意軟體系列，例如 DanaBot 和 RedLine 竊取程式。

4. HijackLoader 背後的攻擊者首選的滲透方法是網路釣魚攻擊，網路犯罪分子會製作看似來自合法來源的電子郵件，希望誘騙收件者打開惡意附件或點擊受感染的連結(如飯店攻擊案)。

5. HijackLoader 變種採用複雜的技術來增強其複雜性和強化迴避偵測能力。

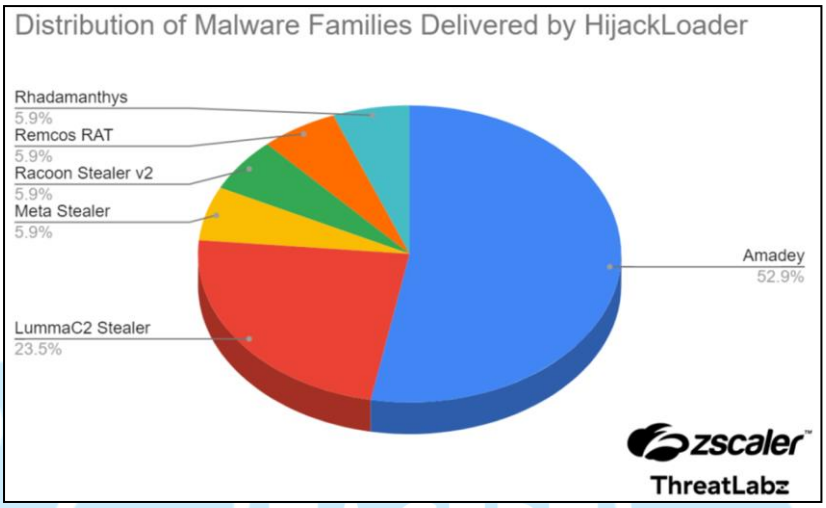
   (1) 將惡意程式及相關工具加入 Microsoft Defender 的白名單。

   (2) 繞過使用者帳號控制（UAC）。

(3) 採用處理程序挖空（Process Hollowing）手法。

(4) 針對端點防護軟體經常使用的內部 API 掛鉤進行迴避。

6. 2024 年 3 月 ThreatLabz 研究人員分析了約 50 個 HijackLoader 樣本，來確定 HijackLoader 目前散播的是哪些惡意軟體，其中以 Amadey 被散播的比例最高。



(資料來源:https://www.zscaler.com/blogs/security-research/hijackloader-updates#indicators-of-compromise--iocs-)

HijackLoader 散播的惡意軟體如下:

(1) Amadey:該木馬能收集有關受害者系統的資料並能夠下載其他惡意軟體。Amadey 為 HijackLoader 散播時所提供的最受歡迎之惡意軟體，佔觀察到的實例的 52.9%，明顯高於其他惡意軟體。

(2) Lumma Stealer (aka LummaC2 Stealer):資訊竊取程式,從加密貨幣錢包、Steam 帳戶、KeePass、FileZilla 和瀏覽器擴充功能等項目中竊取資料。

(3) Racoon Stealer v2:資訊竊取程式，竊取已儲存的密碼、cookie、自動填入資料和加密貨幣錢包等資料。

(4) Remcos:遠端存取木馬 (RAT) 用於取得受害者系統的後門存取權限。

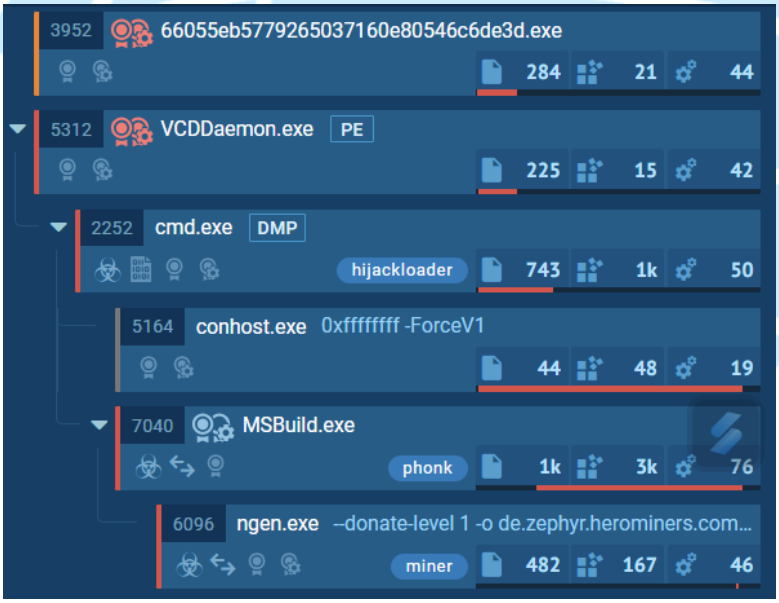
(5) Meta Stealer：針對瀏覽器、加密貨幣錢包、錢包擴充功能和 Steam

帳戶的資訊竊取程式，與 Redline Stealer 有許多相似之處。

(6) Rhadamanthys：為針對錢包、電子郵件、記事應用程式和留言等資訊的竊取程式。

二、 事件檢測

1. 在 AnyRun 沙箱環境下，執行樣本 66055eb5779265037160e80546c6de3d.exe(MD5:66055eb5779265037160e80546c6de3d)。此樣本結合 hijackloader、loader、miner 與 phonk 等特性。它經 Virustotal 檢測其惡意比例為 57/73。在它執行後會呼叫 VCDDaemon.exe，而 VCDDaemon.exe 會呼叫 cmd.exe 來執行 conhost.exe 與 MSBuild.exe。最後 MSBuild.exe 執行後會呼叫 ngen.exe 來執行。



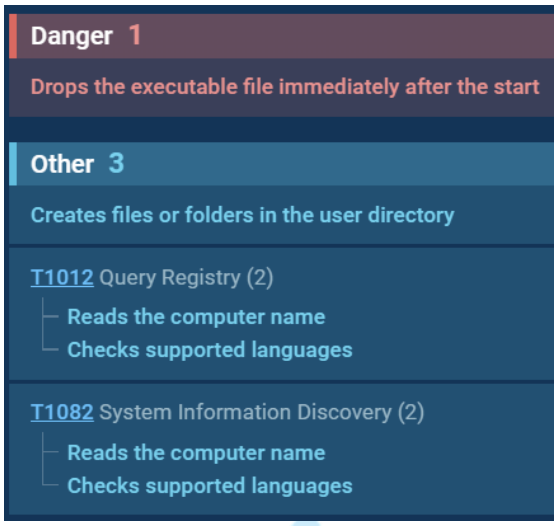
2. 66055eb5779265037160e80546c6de3d.exe 執行後會有下列行為:

(1) 開始執行後立即刪除自己。

(2) 在使用者目錄中產生相同樣本檔案或資料夾。

(3) 讀取電腦名稱。

(4) 檢查支援的語言。



3. VCDDaemon.exe 執行後會有下列行為:

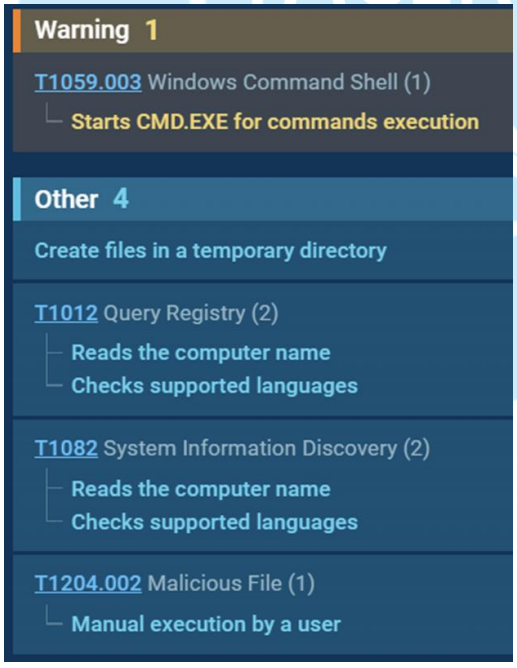
(1) 啟動 CMD.EXE 執行指令。

(2) 在暫存目錄中建立檔案。

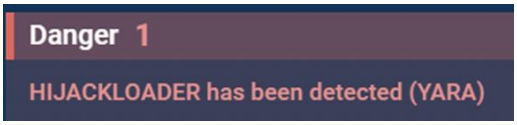
(3) 讀取電腦名稱。

(4) 檢查支援的語言。

(5) 由使用者手動執行它。



4. cmd.exe 執行後會有下列行為:被檢測到為 HijackLoader。



5. MSBuild.exe 執行後會有下列行為:

(1) 連線到 CnC 伺服器。(目的 IP:89.208.107.12:80)

(2) 被檢測到為 PHONK 。

(3) 連線到沒有主機名稱的伺服器。(http[://]89.208.107.12/BEBRIK.php)

(4) 在使用者目錄中建立檔案或資料夾。

(5) 檢查代理伺服器資訊。

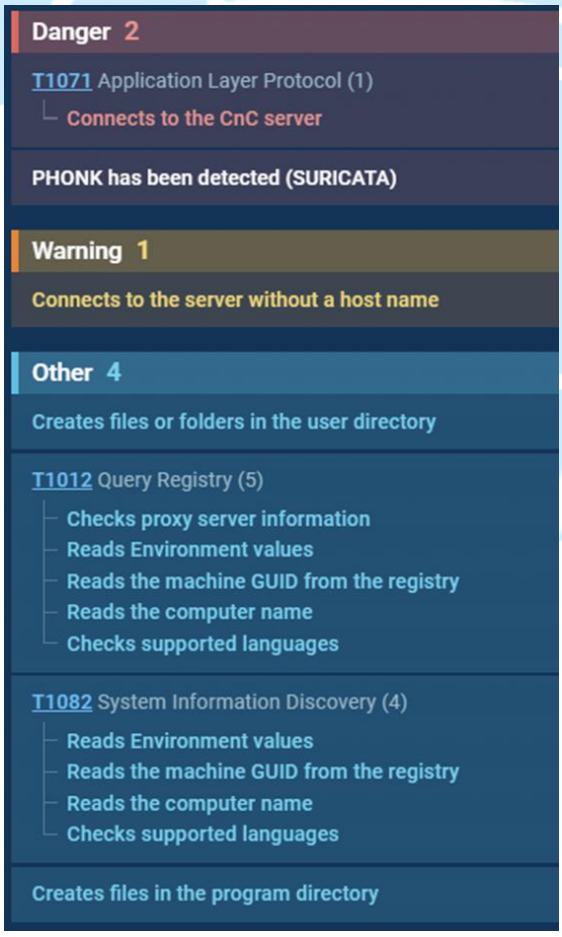
(6) 讀取環境數值。

(7) 從登錄檔中讀取機器 GUID。

(8) 讀取電腦名稱。

(9) 檢查支援的語言。

(10) 在程式目錄中建立檔案。



6. ngen.exe 執行後會有下列行為:

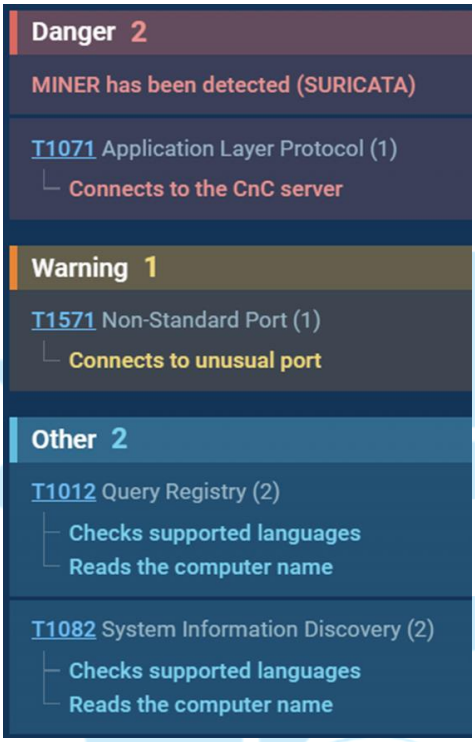
(1)被檢測到為 MINER。(目的 IP:141.95.45.234:1123)

(2)連接到 CnC 伺服器。(目的 IP:141.95.45.234:1123)

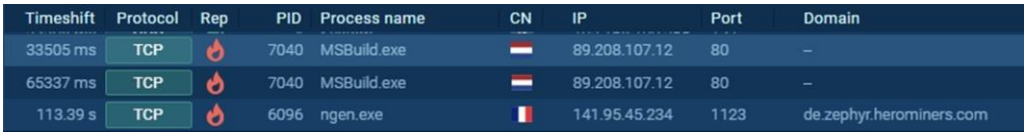
(3)連接到異常連接埠。(port:1123)

(4)檢查支援的語言。

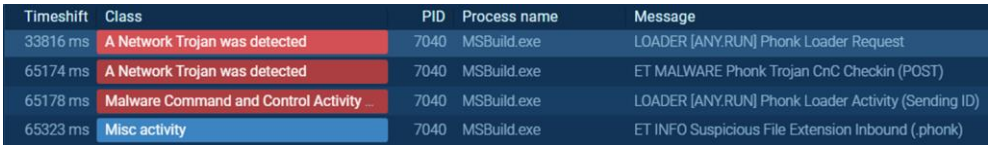
(5)讀取電腦名稱。



7. 檢視對外連線情形，發現會連線兩個目的 IP:89.208.107.12(荷蘭)與 141.95.45.234(法國)。http[://]89.208.107.12/BEBRIK.php 經 Virustotal 檢測其惡意比例為 7/92，為 Phonk C2。141.95.45.234 經 Virustotal 檢測其惡意比例為 1/90 ，可能為礦池。



Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain
33505 ms	TCP		7040	MSBuild.exe		89.208.107.12	80	–
65337 ms	TCP		7040	MSBuild.exe		89.208.107.12	80	–
113.39 s	TCP		6096	ngen.exe		141.95.45.234	1123	de.zephyr.herominers.com



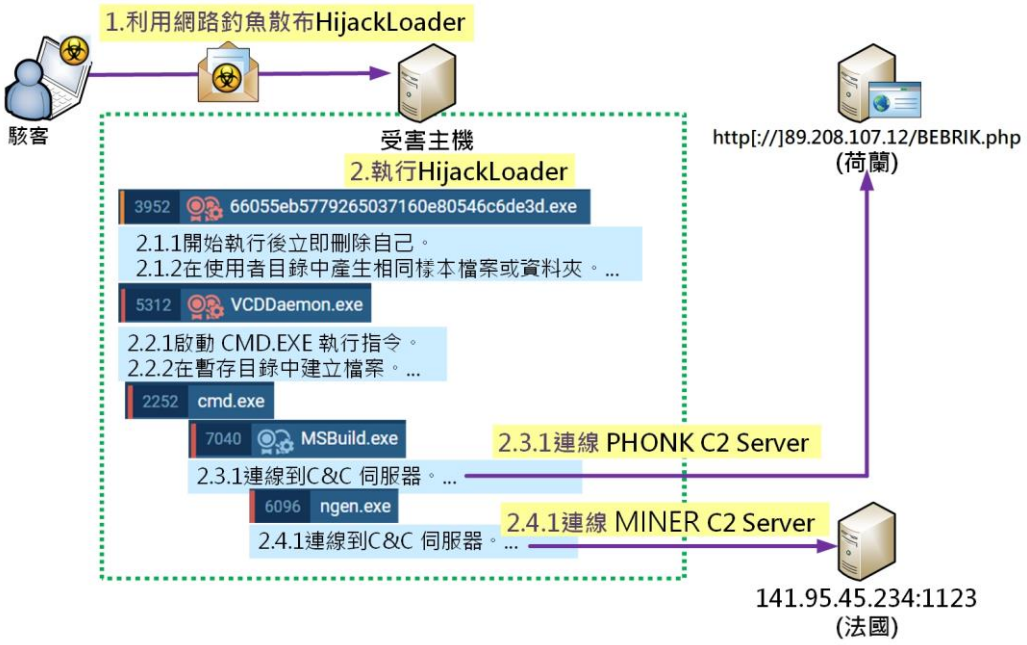
Timeshift	Class	PID	Process name	Message
33816 ms	A Network Trojan was detected	7040	MSBuild.exe	LOADER [ANY.RUN] Phonk Loader Request
65174 ms	A Network Trojan was detected	7040	MSBuild.exe	ET MALWARE Phonk Trojan CnC Checkin (POST)
65178 ms	Malware Command and Control Activity ...	7040	MSBuild.exe	LOADER [ANY.RUN] Phonk Loader Activity (Sending ID)
65323 ms	Misc activity	7040	MSBuild.exe	ET INFO Suspicious File Extension Inbound (.phonk)

Timeshift	Class	PID	Process name	Message
113.36 s	Crypto Currency Mining Activity Detected	2092	svchost.exe	ET COINMINER Observed DNS Query to herominers Domain (h...
113.37 s	Potential Corporate Privacy Violation	6096	ngen.exe	ET POLICY Cryptocurrency Miner Checkin
113.40 s	Potential Corporate Privacy Violation	6096	ngen.exe	ET POLICY Cryptocurrency Miner Checkin

8. 以 MITRE ATT&CK Matrix 分析 HijackLoader，發現該樣本所運用技術橫跨 Execution、Discovery 與 C&C 等 3 個階段，其中包含查詢登錄檔內容、連線 C & C Server。

三、 事件攻擊行為

經由樣本檢測可歸納出 HijackLoader 的攻擊行為如下圖所示，當駭客透過網路釣魚散播 HijackLoader 後，一旦受害主機受感染會陸續下載所搭配的惡意程式，並且也會連線 C2 Server。HijackLoader 載入程式利用 CMD 執行命令程式來隱藏在偵測雷達之下。反過來，它啟動 MSBuild 程式，該程式下載並執行 Phonk，從而下載挖礦程式。 HijackLoader 展示了規避功能，有助於不被某些安全軟體檢測到。



四、 總結與建議

1. 經由 AnyRun 沙箱得知，HijackLoader 透過網路釣魚感染受害主機後，可以下載不同類型的惡意軟體，如本案散播挖礦程式與 PHONK ，而且它也會對外連線兩個 C2 Server。由於它刪除自己後在背景程式中默默執行，不易被發現，加上可搭配不同類型的惡意軟體，將造成不小的資安威脅。
2. 在可能影響方面，它會造成的潛在損害因其散播下載的惡意軟體而不同，所以皆可能對 CIA 中任一者造成衝擊。
3. 對於感染 HijackLoader 的主機有下列處理建議提供學校參考。
   (1) 由於它會下載惡意軟體於受害主機上，故建議可先使用防毒軟體對受害主機進行掃毒 。
   (2) 使用網路連線監控工具(如 TCPView 或 Currports 等)，來查看主機是否有連線 C2 Server，以辨別主機是否感染 HijackLoader 與找出其所下載的軟體所在之處。
4. 為避免未來再次發生類似案件，有下列預防措施提供學校參考。
   (1) 定期更新防毒軟體。
   取得最新的病毒碼，以有效即時保護主機之安全。
   (2) 善用防火牆。
   利用防火牆監視和控制流入和流出的網路流量，而啟用防火牆可能有助於阻止惡意連線。
   (3) 警惕電子郵件之下載連結。
   HijackLoader 透過網路釣魚散播。對於從電子郵件所附之連結下載檔案，請謹慎行事。
   (4) 謹慎瀏覽網站。
   攻擊者可能會利用合法的雲端硬碟平台來散播 HijackLoader 和其

他惡意軟體，需密切注意造訪的網站，不要過度信任網站上的任何檔案。

參考資料

1. **HijackLoader Expands Techniques to Improve Defense Evasion**
   https://www.crowdstrike.com/blog/hijackloader-expands-techniques/
2. **Hijackloader**
   https://any.run/malware-trends/hijackloader
3. **HijackLoader Targets Hotels: A Technical Analysis**
   https://alpine-sec.medium.com/hijackloader-targets-hotels-a-technical-analysis-c2795fc4f3a3
4. **HijackLoader Updates**
   https://www.zscaler.com/blogs/security-research/hijackloader-updates#indicators-of-compromise--iocs-