TLP:WHITE

資訊竊取程式 Lumma Stealer 之分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2024 年 08 月

一、事件簡介

1. 根據 ANYRUN 沙箱平台的惡意軟體趨勢追蹤器統計，在 2024/07/12 ~ 2024/08/11 這 30 天內最著名的惡意軟體為 Lumma。在 30 天內有 440 個樣本檢測數量，與第二名 249 個有大差距，可見這期間有許多 Lumma 的攻擊產生。為了了解 Lumma 的攻擊行為，故對其樣本進行檢測作業。

No.	Family	Type	Trand changes	World rank	Tasks overall
1	Lumma	Stealer		1 ↑	814
2	AsyncRAT	RAT		2 ↑	810
3	Agent Tesla	Trojan		3 ↓	734

二、 Lumma Stealer

1. Lumma Stealer(又稱為 LummaC2 Stealer)在 2022 年 08 月首次被發現。
   (1) 它在暗網論壇和 Telegram 管道上，以惡意軟體即服務的形式出售，並提供多種服務方案給買家選擇。
   (2) 它通常針對受感染系統上的加密貨幣錢包、登入憑證和其他敏感資訊進行竊取。
   (3) 它會定期獲取更新，以改進和擴展其功能，使其成為一個嚴重的資訊竊取威脅。
2. 2023 年 11 月資安公司趨勢科技發現駭客透過 Discord 平台來散播 Lumma Stealer。駭客會使用 Discord 的內容派送網路 (CDN) 來儲存及

散播 Lumma Stealer。駭客利用這個社群平台的應用程式開發介面 (API) 來開發機器人程式，用來與惡意程式通訊並進行遠端遙控。這些機器人也會將偷到的資料傳送到私人 Discord 伺服器或頻道。

3. 2024 年 01 月 FortiGuard Lab 發現駭客利用 YouTube 頻道散播 Lumma Stealer。駭客向使用者提供含有惡意網址的安裝指南，並利用 GitHub 和 MediaFire 等開源平台，取代部署自己的惡意伺服器。這些開源平台讓使用者直接下載一個新的私有.NET Loader，來散播變種 Lumma Stealer。在這次攻擊中，駭客使用精心製作的安裝壓縮檔案作為一個誘餌來傳遞惡意程式。巧妙地利用使用者想安裝破解程式的意圖，促使他們毫不猶豫地點擊安裝檔案。整個過程中使用開源平台網址的目的在減弱使用者的警覺性。
4. 2024 年 04 月因假的瀏覽器更新網頁導致了大量惡意軟體感染，其中包括 Lumma Stealer。當使用者瀏覽包含惡意 JavaScript 的受感染網頁時，會觸發注入的惡意 JavaScript 程式碼，從而將使用者引導至虛假的軟體更新網頁，進而下載惡意的 ZIP 更新檔。
5. 2024 年 06 月駭客誘騙使用者下載受密碼保護的檔案，包含 Cisco Webex Meetings 應用程式的木馬副本。當受害者執行安裝檔案時，Cisco Webex Meetings 應用程式會秘密載入程序，從而導致資訊竊取模組程式的執行。
6. Lumma Stealer 對多種電腦系統構成重大威脅。它的主要攻擊目標是執行 Windows 作業系統的裝置。因為它的這種廣泛的兼容性使惡意軟體能夠滲透到龐大的系統網路，從而增加其潛在的影響力。
7. Lumma Stealer 之功能

   (1) 資料外洩

   它能有效地從目標應用程式收集敏感資訊，包括登入憑證、財務資料和個人詳細資訊。

(2) 定期更新

它能定期執行自動更新。

(3) 資料日誌收集

它可從受感染的主機收集詳細的資料日誌，包括從瀏覽器和加密貨幣錢包中提取的資訊。

(4) 載入程式功能

竊取者可以將其他的惡意軟體投放到受感染的主機上，從而擴大它的惡意功能和潛在影響。

Lumma Stealer 具有廣泛的功能，使其成為網路犯罪者的多功能工具。例如，竊取者傳輸的所有資料都在伺服器端解密，這使得在滲透過程中分析惡意軟體的流量變得更加困難。

8. Lumma Stealer 之散播方式

(1) 仿冒軟體

散播 Lumma Stealer 的最受歡迎方法之一是透過假軟體。當毫無戒心的使用者下載並安裝這些虛假應用程式時，他們會將惡意軟體引入他們的系統中。

(2) 網路釣魚電子郵件

網路釣魚電子郵件是廣泛使用的惡意軟體散播攻擊媒介。網路犯罪者製作看似來自合法來源（例如銀行、電子商務平台或社群媒體網路）的電子郵件，來散播 Lumma Stealer。。

(3) Discord 訊息

在某些情況下，Lumma Stealer 攻擊者會透過在聊天平台 Discord 上直接發送訊息來尋找受害者。攻擊者會與受害者接觸，試圖建立信任並說服他們以虛假藉口下載受感染的可執行檔。

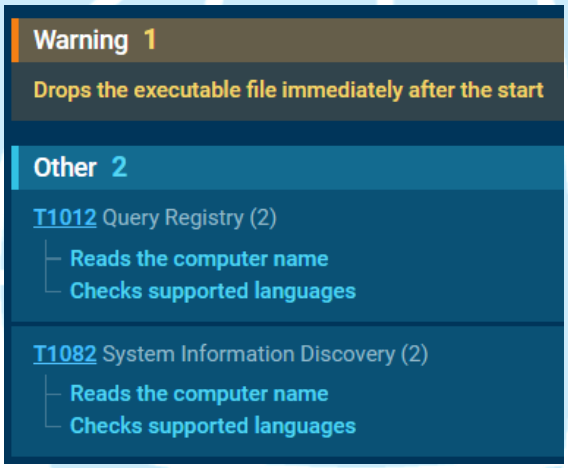
三、 Lumma 樣本檢測

1. 在 ANYRUN 沙箱下檢測 Lumma 樣本 fKYrTm48vZ.exe，它執行後會呼叫 Regasm.exe 來執行，而 Regasm.exe 執行後會呼叫 Werfault.exe 來執行。

(1) fKYrTm48vZ.exe 的 MD5 為 d5c9bbccffc7a6a92b61c567c6a23e81。

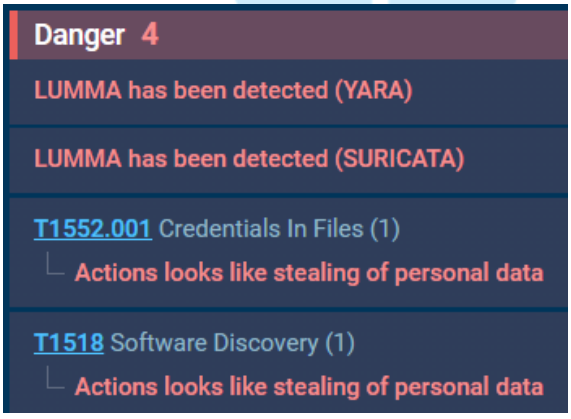
(2) 它執行後會刪除自己本身。

(3) 它會讀取主機名稱與檢查支援的語言。



2. Regasm.exe 執行後會有下列行為。

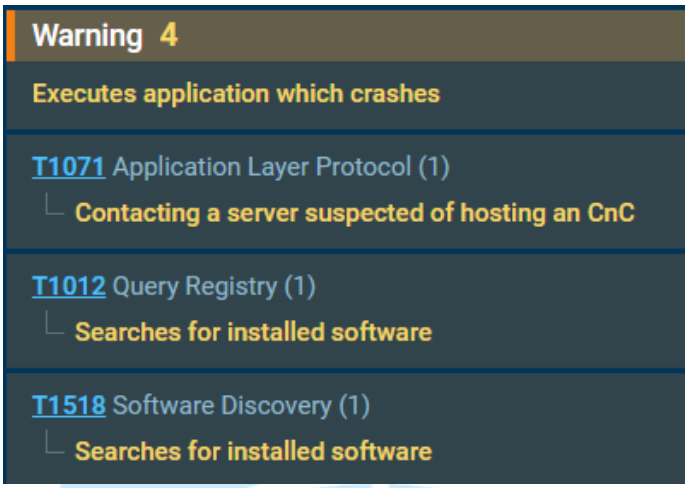
(1) 竊取個人資料。



(2) 執行 WerFault.exe。

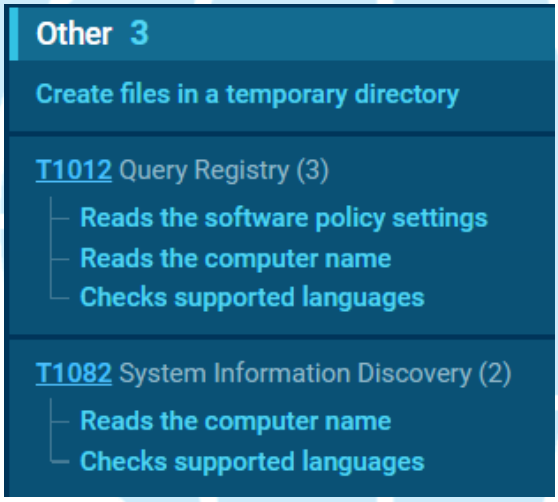
(3) 聯絡 C&C 的伺服器，連線 IP:188.114.96.3 Port:443。

(4) 搜尋已安裝的軟體。



(5) 在暫存目錄中建立檔案。

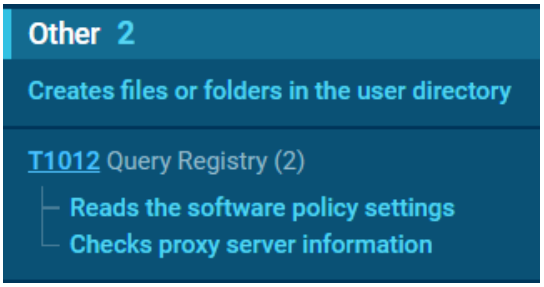
(6) 讀取軟體策略的設定與主機名稱，以及檢查支援的語言。



3. WerFault.exe 執行後會有下列行為。

(1) 在使用者目錄中建立檔案或資料夾。

(2) 讀取軟體策略的設定與檢查代理伺服器的資訊。



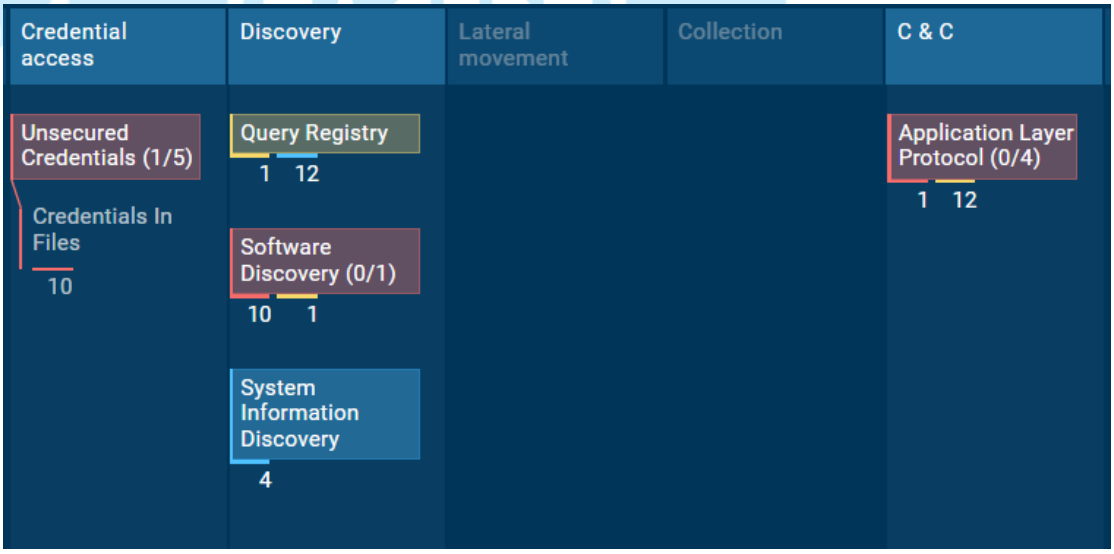
4. 從網路連線發現，Regasm.exe 所連線的美國 IP:188.114.96.3 為一個 C2

Server 的 IP。該 IP 所對應到的網址為 hookybeamngwskow.xyz，是與 Lumma 有關的 C2 網址。該 IP 經 Virustotal 檢測為 3/93，網址 hookybeamngwskow.xyz 經檢測為 10/93。

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
6747 ms	TCP		6476	RegAsm.exe		188.114.96.3	443	hookybeamngwskow.xyz	CLOUDFLARENET	↑ 21.4 Kb ↓ 4.11 Kb
6750 ms	TCP		6476	RegAsm.exe		188.114.96.3	443	hookybeamngwskow.xyz	CLOUDFLARENET	↑ 1.89 Kb ↓ 4.12 Kb
7256 ms	TCP		6476	RegAsm.exe		188.114.96.3	443	hookybeamngwskow.xyz	CLOUDFLARENET	↑ 372 Kb ↓ 4.10 Kb

5. IP:188.114.96.3 屬於 Cloudflare CDN(內容派送網路)的 IP，在 AbuseIPDB 上被檢舉 508 次，它首次被檢舉於 2023 年 12 月 21 日。最近一次被檢舉是在 2024 年 08 月 09 日被檢舉有網路釣魚行為，可見它可能仍被濫用中。

6. 以 MITRE ATT&CK Matrix 分析 Lumma，發現該樣本所運用技術橫跨 Credential access 、Discovery 與 C&C 等 3 個階段，其中包含竊取個人資料、連線 C&C Server。

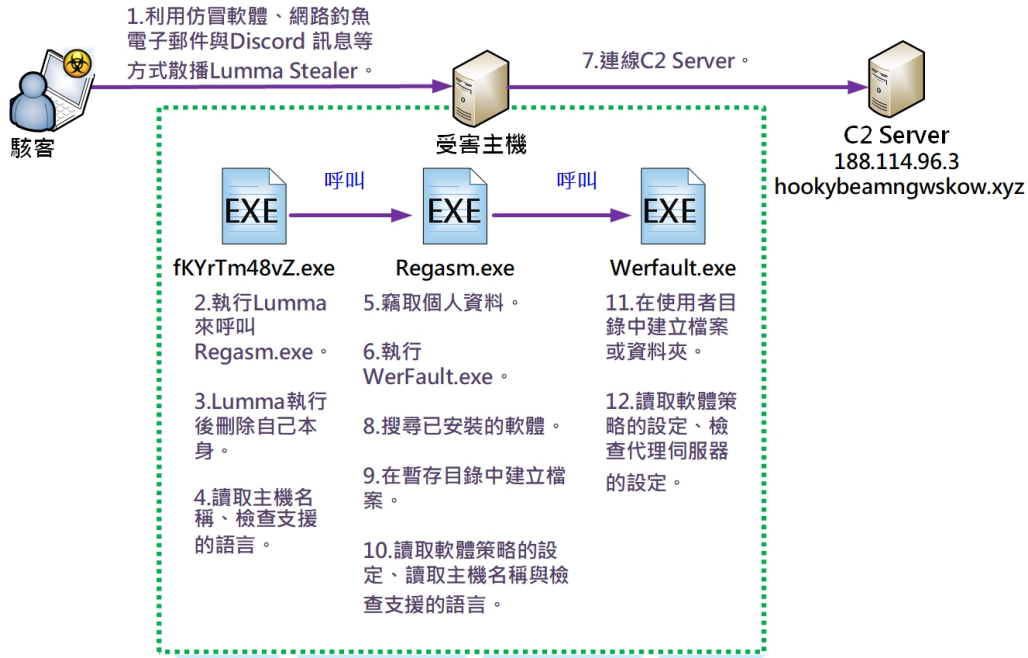


四、 事件攻擊行為

由 Lumma 攻擊行為可畫出下面攻擊行為示意圖，一開始駭客利用仿冒軟體、網路釣魚郵件與 Discord 訊息等方式來散播 Lumma。當主機執行 Lumma 時會呼叫 Regasm.exe 來執行，接著 Regasm.exec 執行後會呼叫

WerFault.exe。在這些程式執行期間，它會刪除自己本身、讀取主機名稱、檢查支援的語言、竊取個人資料、連線 C2 Server、搜尋已安裝的軟體、在暫存目錄中建立檔案、讀取軟體策略的設定、在使用者目錄中建立檔案或資料夾，以及檢查代理伺服器的設定等行為。

因為駭客想隱藏攻擊行為，所以 Lumma Stealer 的執行鏈就盡可能地保持簡單，導致在受害主機上沒有太多程序，也沒有使用到系統工具。當 Lumma 感染主機後會立即開始執行，它的唯一程序是負責執行所有的攻擊行為，包括竊取資料與連線 C2 Server。



五、 總結與建議

1. Lumma Stealer 能夠從受害者主機中竊取敏感資料，它針對系統資訊、瀏覽器、加密錢包和瀏覽器擴充程式進行攻擊。為了規避檢測和分析，它使用多種混淆技術。它會與 C2 伺服器建立連線，以達成指令交換並傳送所竊取的資料， 並且透過連線能自動更新程式。
2. 在可能影響方面，它會造成的潛在損害如下：資料竊取、遠端控制、隱私洩漏，所以會對 CIA 中的「機密性」造成衝擊。

3. 在處理方式方面，有下列兩點建議提供參考。
   (1) 在處理本類攻擊事件時，使用者可先使用防毒軟體對受害主機進行掃描。
   (2) 使用 TCPView 或 CurrPorts 等網路連線監控工具，來查看主機是否有連線 C2 Server，以辨別主機是否感染 Lumma 與找出其所在之處。
4. 由於 Lumma Stealer 的威脅日益嚴重，需要採取積極主動的網路安全方法。隨著它變得越來越普遍，個人和組織必須了解其多樣化的散播方法並採取保護措施。在防範措施方面，有五點建議如下提供參考。
   (1) 不從未知來源下載和執行軟體。
   (2) 不隨意開啟郵件的附件或點選不明的連結。
   (3) 定期檢視主機上是否有不明的網路連線。
   (4) 不在惡意軟體常用的路徑上建立 PE 檔案（例如：%PROGRAMDATA%）。
   (5) 定期更新病毒碼並使用防毒軟體掃毒，以防範惡意威脅。

參考資料

1. Fortinet 詳細揭露駭客組織利用 YouTube 散播 Lumma 變種攻擊手法
https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=10898
2. Fake Browser Updates delivering BitRAT and Lumma Stealer
https://www.esentire.com/blog/fake-browser-updates-delivering-bitrat-and-lumma-stealer
3. 小心：Lumma Stealer 資訊竊取程式透過 Discord CDN 散播
https://www.trendmicro.com/zh_tw/research/23/k/beware-lumma-stealer-distributed-via-discord-cdn-.html
4. Lumma
https://any.run/malware-trends/lumma
https://app.any.run/tasks/7c6cf961-3516-4855-8b81-db67169a026d