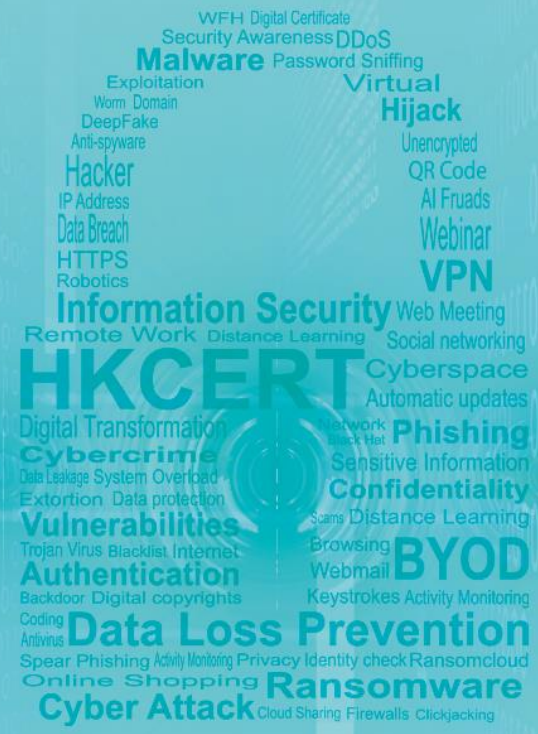
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2022 第四季度

發佈日期: 2023年3月



前言

提升資訊保安由認知做起

現今，有很多具備上網功能的數碼設備(例如個人電腦、智能手機、平板裝置等)，在用戶不知情下被入侵，令儲存在這些設備內的數據，每天要面對被盜取和洩漏，甚至可能被用於進行不同形式的犯罪活動的風險。

《香港保安觀察報告》旨在提高公眾對香港被入侵系統狀況的認知，從而作出更好的資訊保安選擇。這份季度報告提供的數據聚焦在被發現曾經遭受或參與各類型網絡攻擊活動（包括網頁塗改、釣魚網站、殭屍電腦等)的香港系統，其定義為處於香港網絡內，或其主機名稱的頂級域名是「.hk」或「.香港」的系統。報告亦會回顧該季度所發生的重大保安事件及探討熱門保安議題，並提出易於執行的保安建議，提升公眾的資訊保安認知的水平，增強應對有關風險的能力。

善用全球保安資訊力量

本報告是香港電腦保安事故協調中心 (HKCERT) 和全球各地資訊保安研究人員共同合作的成果。很多資訊保安研究人員具有偵測針對他們或其客戶攻擊的能力，有些會把攻擊來源的可疑 IP地址或惡意活動網絡連結的數據資料收集起來，並提供給其他資訊保安機構，以改善互聯網的整體保安。他們會遵守良好的作業守則，在分享數據前，先刪除個人身份資料。

HKCERT 建立Information Feed Analysis System (IFAS) 系統，收集和匯聚這些數據，對有關香港的資料進行分析。數據的來源廣泛和可靠，可以持平地反映香港資訊保安情況。

HKCERT會移除來自多個數據來源的重複報告，並以下面的統計指標來確保統計數據的質量：

網絡攻擊類型	統計指標
網頁塗改、釣魚網站	在本報告所述期間，錄得有關的單一網址的數量
殭屍電腦	在本報告所述期間，錄得各個殭屍網絡在季度內的同日單一IP 地址數量的最高值的總和

以下是IFAS資料的來源:

網絡攻擊類型	資料來源	開始使用
網頁塗改	Zone – H	2013-04
釣魚網站	CleanMX – Phishing	2013-04
釣魚網站	Phishtank	2013-04
殭屍電腦	Shadowserver - microso _sinkhole_events	2021-06
殭屍電腦	Shadowserver - microso _sinkhole_http_events	2021-06
殭屍電腦	Shadowserver - sinkhole_http_events	2021-06
殭屍電腦	Shadowserver - sinkhole_events	2021-06
殭屍電腦	Shadowserver - honeypot_darknet_events	2021-06

本中心採用以下方法去識別網絡的地理位置是否在香港。

方法名稱	開始使用	最後更新
Maxmind	2013-04	2023-01

更好的資訊帶來更好的服務

HKCERT將來會加入更多有價值的數據來源以進行更深入的分析，持續改善報告內容，亦會探討如何最有效利用這些數據提升 HKCERT 的服務。請電郵至*hkcert@hkcert.org* 反饋閣下的意見。

報告的局限

本報告的數據來自多個途徑，他們有不同的來源、收集週期和表達方式，各自亦存有局限，因此數據只宜作為參考，不宜用作直接比較或視為反映現實的全貌。

免責聲明

本中心可隨時更新或修正報告，恕不另行通知。對於本報告內容及數據中出現的任何錯誤、偏頗、疏漏或延誤，或據此而採取之任何行動，本中心概不負上任何責任。對於因使用本報告內容及數據而產生的任何特殊的、附帶或相應的損失，本中心概不負上任何責任。

授權條款

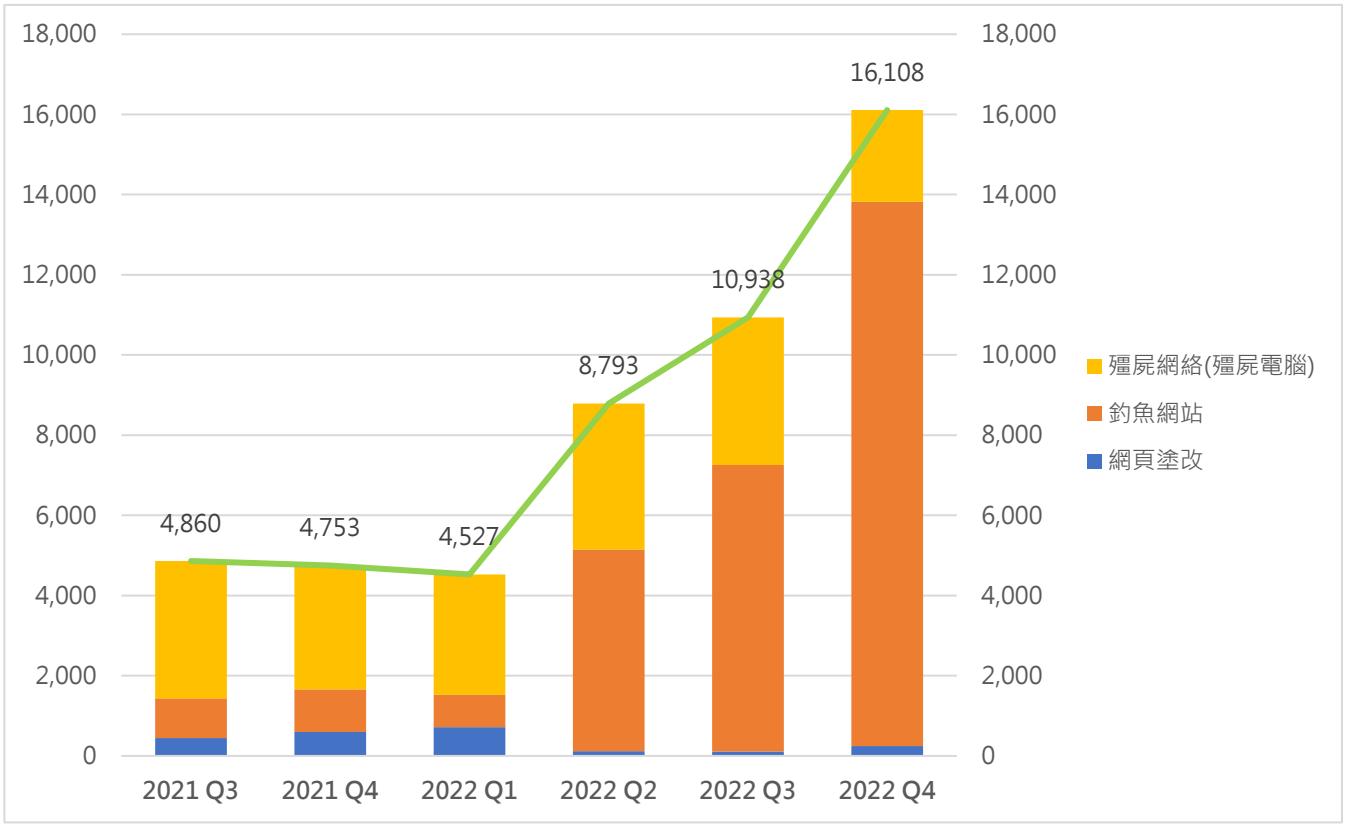
2022 第四季度報告概要

涉及香港的單一網絡保安事件宗數

16,108

按季上升

↑47%



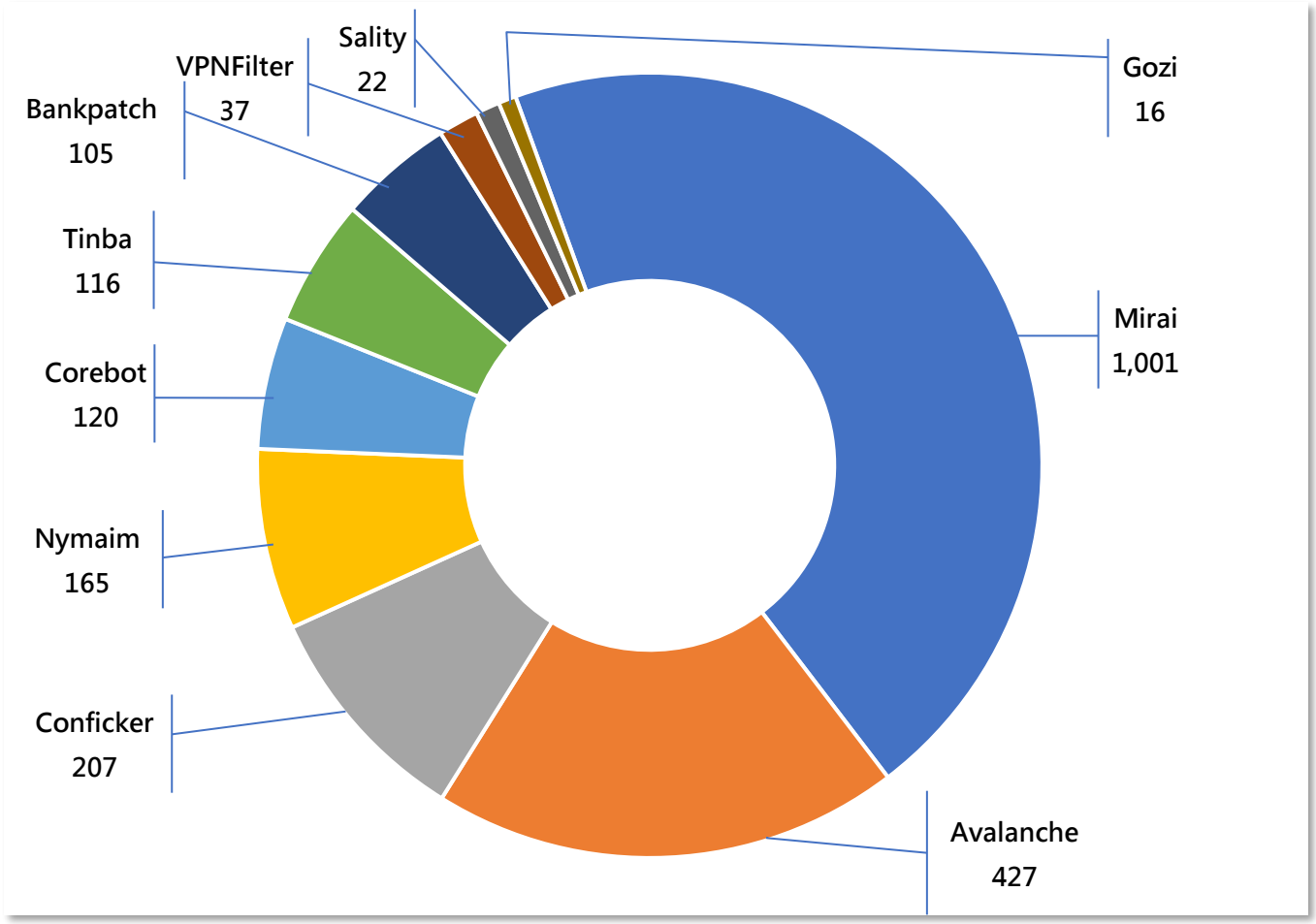
事件類別	2021 Q4	2022 Q1	2022 Q2	2022 Q3	2022 Q4	按季
網頁塗改	595	718	118	113	249	+120%
釣魚網站	1,061	806	5,033	7,141	13,574	+90%
殭屍網絡(殭屍電腦)	3,097	3,003	3,642	3,684	2,285	-38%
總數	4,753	4,527	8,793	10,938	16,108	+47%

香港網絡內的主要殭屍網絡

Mirai
1,001
↓ 31.8%

Avalanche
427
↓ 47.8%

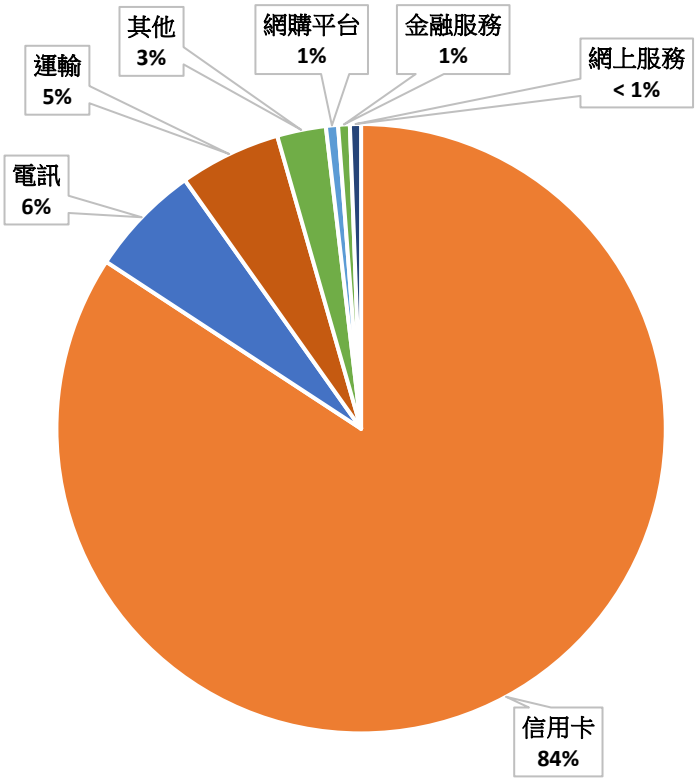
Conficker	207	-7.2%
Nymaim	165	-48.1%
Corebot	120	+421.7%
Tinba	116	-64.8%
Bankpatch	105	+54.4%
VPNFilter	37	-15.9%
Sality	22	-88.5%
Gozi	16	+14.3%



** 主要殭屍網絡指在報告時間內，透過資訊來源有可觀及持續穩定的數據。殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的單一IP地址總數的最大值。換言之，由於不是所有殭屍電腦都會在同一天開機，因此殭屍網絡的實際規模應該比以上的數字更大。*

網絡釣魚事件超越1萬宗！公眾須加強警剔 提防受騙

釣魚網站事件連升三季，並首次錄得過萬宗，按季激升90%，較去年同期上升逾11倍。數據顯示，84%的釣魚網站為虛假信用卡公司網站；6% 和 5% 與電訊和運輸行業相關。雖然於報告撰寫時，抽樣測試結果顯示這些網站均已關閉或不能進入，但相信黑客有意通過相關網站騙取用戶的信用卡或其他個人信息，用於非法行為。



一般市民認識的釣魚網站往往是透過電郵中的超連結被引導至黑客塑造的虛假網站，繼而誘騙受害者輸入相關的登入名稱、密碼及其他個人資料等。隨後，黑客會利用相關資料進行不法行為，例如盜取存款或借貸。

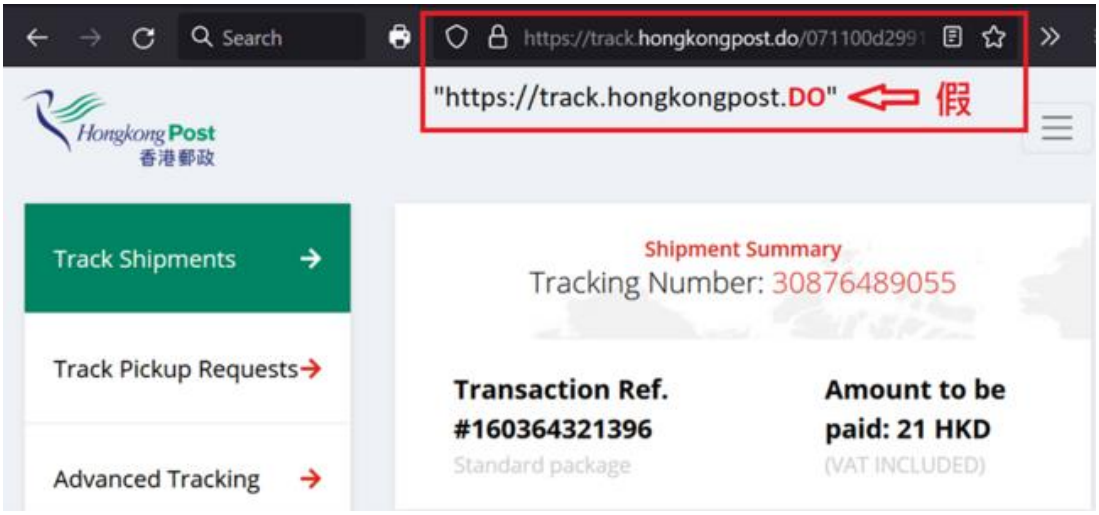
然而，近期有市民報稱在電話中收到來自某大型超市的短訊並指示用戶按下短訊內的超連結，而短訊上款名稱是該機構名稱，而且過往的訊息也是用戶曾經按入或使用過。那麼是手機壞了？是黑客駭入自己手機？還是黑客駭入了該機構？黑客這手法的確令市民真假難分，難以辨認來源，稍有不慎按入會成為黑客的目標。由於黑客會一直不斷改良這些攻擊手法，意圖讓更多人受騙，因此 HKCERT 今次特別介紹針對網上購物的釣魚攻擊手法，並帶出大家網上消費時必須注意的地方，以免陷入此類網絡釣魚陷阱。

釣魚訊息

最近常見的網絡釣魚攻擊手法主要是透過智能手機系統內置及第三方的即時通訊應用程式，將存有釣魚網站的惡意縮寫URL連結以訊息發送至收訊人。由於大多數通訊軟件都可以設定發件人的名稱，因此黑客可以偽裝成真實品牌的名稱。以下是一些網絡釣魚攻擊發出的訊息示例。

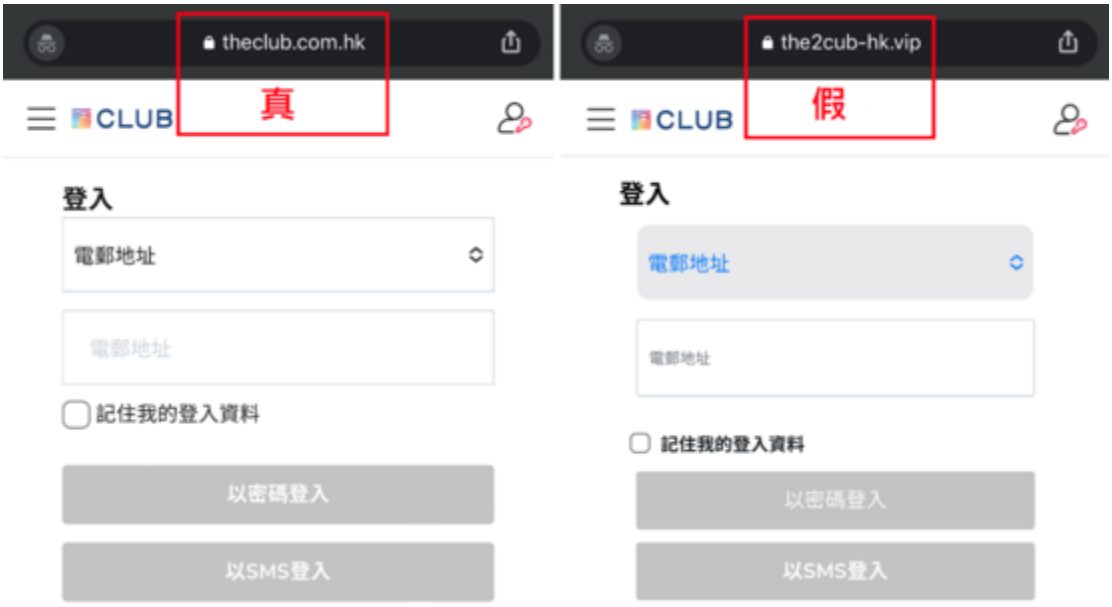
與真實網站相似的釣魚網站

為了誘使受害者認為釣魚網站是官方網站並繼續輸入資料，黑客會註冊與該品牌網站相似的域名。 例如: 香港郵政的正確域名為 “hongkongpost.hk” ，但黑客寄存了釣魚網站在 “hongkongpost[.]do” 的域名中。



複製真實網頁介面的釣魚網頁

除了使用與真實網頁相似的域名和 URL 連結外，黑客最近還會複製真實網站的網頁介面，例如其登錄頁面。此方法會節省設計網絡釣魚頁面的時間，因此大多數黑客會從真實網站中複製網頁介面後再更改網頁後端設置使用。此舉會讓用戶更難分辨瀏覽的網頁真確性。



社交媒體平台中的網絡釣魚頁面

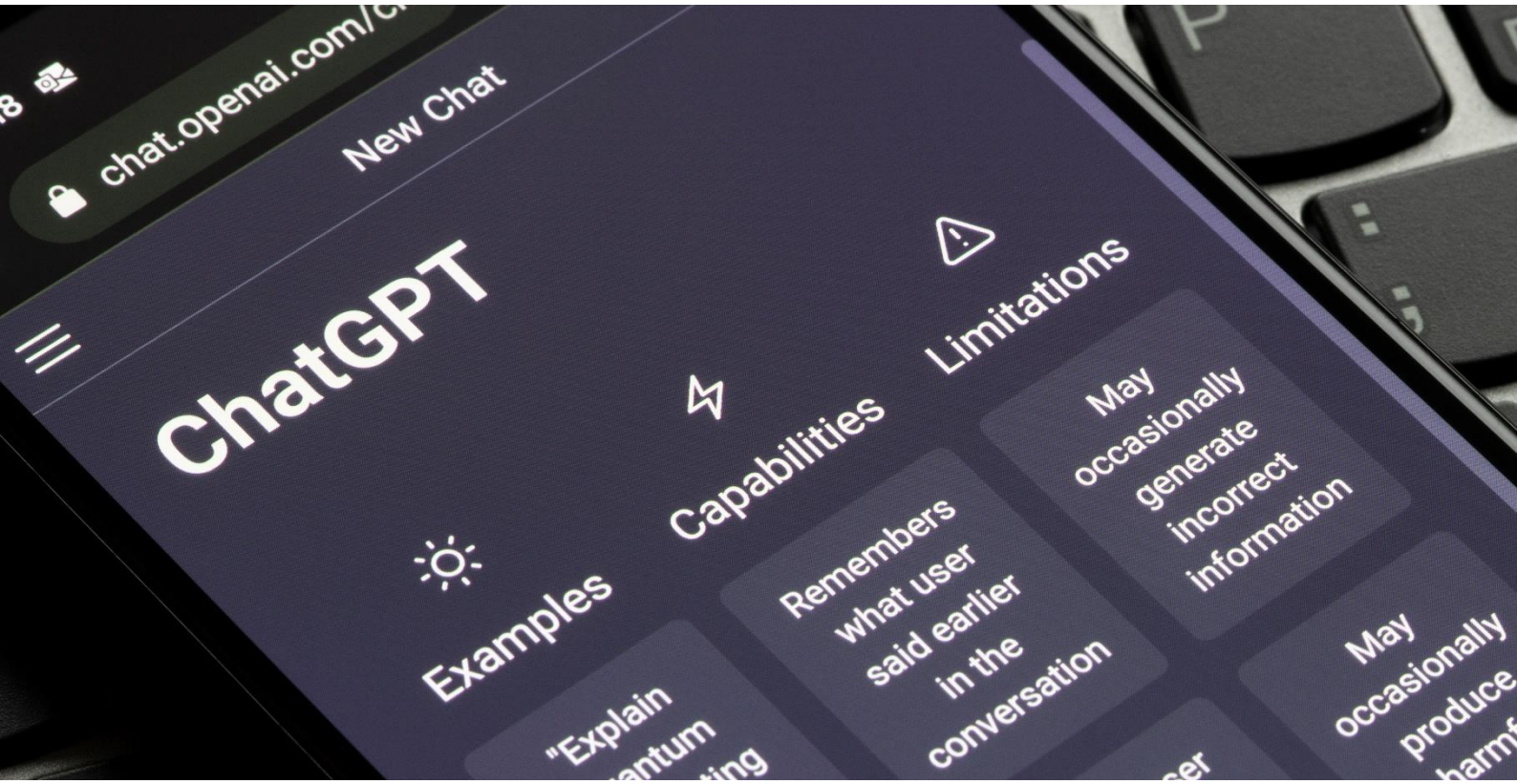
隨著公眾廣泛使用 Facebook、Instagram 等社交平台，一些黑客也會在社交平台上創建虛假頁面。他們大多會在頁面中發布一些虛假的優惠活動，並附上釣魚網站的連結。

下圖是由黑客創建的 HKTVmall Facebook 專頁，其設計與 HKTVmall 官方 Facebook 社交專頁非常相似；另一張圖則是 HKTVmall 的真實 Facebook 專頁頁面，並帶有 Facebook 認證的藍色徽章。

網上購物安全貼士

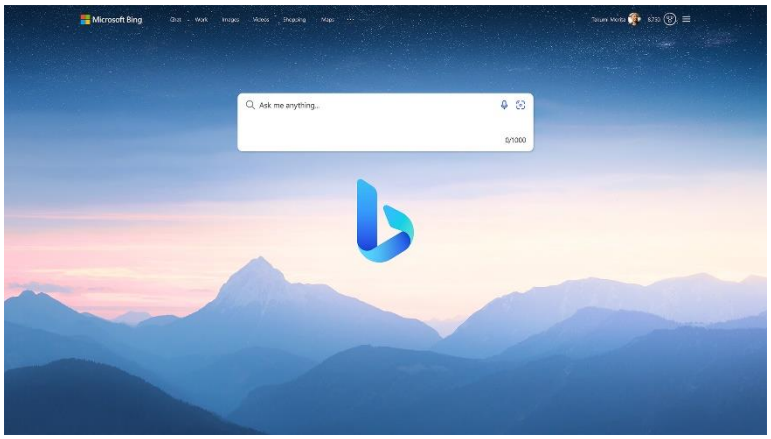
1. 切勿隨便點擊來歷不明的連結或附件。盡量在瀏覽器直接輸入網購平台網址或使用瀏覽器書籤。檢查連結及電郵的合法性，例如檢查清楚網址有否拼寫錯誤、文法錯誤或寄件人是否可信。若網站並非使用 HTTPS 加密，應倍加小心，切勿在沒有加密的情況下輸入敏感資訊；
2. 定期轉換網購平台賬戶密碼，於不同的帳戶使用不同的密碼，以防止其中一個資料被外洩後牽連其他帳戶；
3. 用戶應啟用多重認證以加強保安；
4. 只經官方網站或手機應用程式購物或查看訂單情況；
5. 收到可疑電郵或訊息後，可以向官方渠道查詢詳情，切勿向來歷不明的電郵或訊息發送者提供敏感資料；
6. 定期檢查自己的網上付款記錄，查看是否有可疑交易；
7. 使用社交平台徽章認證功能（例如 Facebook 和 Instagram 中的藍色徽章）來驗證網店的社交平台頁面是否真實；
8. 在瀏覽器上設定反釣魚網站功能以助阻擋釣魚攻擊；和
9. 使用「CyberDefender 守網者」提供的免費搜尋器「防騙視伏器」來辨識詐騙及網絡陷阱，此搜尋器支援檢查電郵地址、網址和 IP 地址等。

網絡焦點：用人工智能找答案 多角度查證保平安



近日人工智能（AI）聊天機器人ChatGPT在互聯網上火紅，據報導已有一億用戶，大部份使用者都表示相比起傳統搜尋引擎只依據輸入的查詢來提供相關度高的網站，ChatGPT能讓用戶以人與人對話的方式提問然後輸出回應，加上生成的答案十分精準及附有詳細解釋，省卻用搜尋引擎後還要自行查閱資料的時間。

雖然其開發者OpenAI表示免費版ChatGPT仍在研究預覽階段，但其受歡迎程度卻標誌著將AI及機器學習技術呈現至普羅大眾面前的重大成功。近日各大資訊科技公司都相繼公布會把AI整合到其網上服務的計劃：例如Microsoft會把比ChatGPT更強大的AI技術與搜尋引擎Bing及瀏覽器Edge整合；另一搜尋引擎巨頭Google亦將於未來數周把其對話式AI服務Bard逐步加入到其產品中。可見不久將來會有更多AI技術整合到不同的網上服務，涉足大家的日常生活。

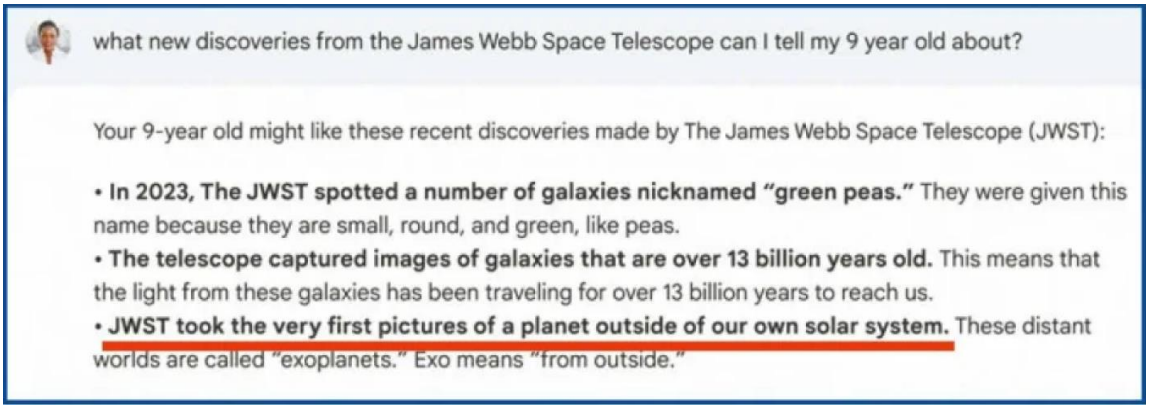


AI的普及應用，一方面讓大家工作或生活上更省時便利，例如有人已利用ChatGPT編寫程式或文章，能得出比真人更快、更少錯誤的程式，生成的文章內容亦很豐富及井井有條；另一方面，亦曾有不法分子利用ChatGPT製作釣魚郵件內容，甚至編寫惡意程式，縱使官方已加入保安機制禁止生成惡意內容，但已有網絡犯罪份子開發規避方法，並以網絡犯罪服務方式販賣，由此可見潛在保安問題亦不容忽視。

HKCERT在2023年2月舉行的最新一次年度資訊保安展望簡布會上亦預測利用AI的攻擊及網絡犯罪服務將會是2023年五大資訊保安風險之一，當中更羅列多種不法分子如何利用AI進行攻擊的可能情況，除上述提到的例子外，還包括AI欺詐及毒害AI模型。總結AI涉及的保安風險有以下幾種：

- 數據私隱和保密：AI需要大量數據進行訓練，其中可能包括敏感信息，如個人詳細信息、財務信息和醫療記錄。這可能引發私隱問題，因為有關的AI模型可能會訪問和生成敏感信息。

- 錯誤訊息：AI為求產生的結果有連貫性及通順，可能會編造虛假或誤導性訊息，用戶慣性倚賴AI生成的資料可能會對事實有錯誤的認知。另外，訊息的準確性亦會受到其所接受的訓練數據影響，例如ChatGPT的訓練數據止於2021年，所以當問到誰是最近的世界盃冠軍時，它會回答法國 (2018年冠軍)，而不是阿根廷(2022年冠軍)；其他錯誤訊息的例子包括在Google宣傳其聊天機器人Bard的廣告中，被發現它在回答有關「詹姆斯韋伯太空望遠鏡」的問題中包含錯誤的資訊。



- **偏見問題：AI的訓練數據可能來自互聯網，當中資料或包含偏見和歧視成份。從而導致AI模型產生偏頗和帶有歧視成份的回應。此外，不法分子亦可利用偏頗的數據，訓練AI模型，令AI生成惡意的回應，此手法稱為「對抗性干擾」。**

- **版權問題：考慮第三方的權利都是很重要，例如由ChatGPT輸出的回應中可能涉及擁有受版權保護資料的人士。侵犯他人的權利，包括未經許可使用其受版權保護的資料，可能會導致法律責任。因此使用ChatGPT時，要考慮和尊重其開發者和其他人的知識產權，並確保對 ChatGPT 的回應作任何使用都符合法律規定。**

其實AI是一個中性的工具，本身並沒有對錯。正如當大家用ChatGPT問其自身是否存在保安隱憂時，ChatGPT的最後回應是：" However, it is important for users and developers to be aware of these security concerns and take appropriate measures to mitigate them." ，這說明了最終責任應該落在用家本身。最後，當大家使用AI時，應該保持凡事核查的心態，從多個源頭查證事實。

HKCERT 資安小貼士：企業要時刻做好系統保安更新 免讓客戶資料成網絡釣魚材料

本地連鎖沖印店快圖美於去年10月遭勒索軟件攻擊，資料被惡意存取及加密，超過六十萬客戶資料外洩，當中包括姓名、性別、出生日期、電話號碼、電郵地址、聯絡地址及送貨地址。個人資料私隱專員公署近日就事故發表調查報告，指快圖美沒有做好個人資料保安措施，違反《私隱條例》，向該機構送達執行通知，指示其糾正和防止違規情況再發生。

調查發現

快圖美於2018年所購買的防火牆於翌年啟用保密插口層虛擬私有網絡（SSL VPN）後，防火牆的生產商已發現這SSL VPN功能存在保安漏洞及發出警告，呼籲用家即時停用，直至更新作業系統和重設所有帳戶密碼，並且建議啟用多重認證。可是，當時快圖美並無即時更新系統，最終導致黑客成功利用該漏洞入侵系統，令客戶資料外洩。

今次事故反映要時刻做好系統保安的重要性，當得悉出現潛在威脅後，要馬上作出相應的跟進行動，絕不能掉以輕心，因此系統管理員需留意以下要點來加強系統保安：

1. 要保持軟件、作業系統及防毒軟件更新及定期安裝修補程式，尤其是暴露於互聯網上的系統（例如：防火牆、VPN伺服器等）；
2. 避免使用生命週期已結束的產品；
3. 啟用多重認證保護網路及系統管理員帳戶；
4. 可參考HKCERT的《中小企保安事故應變指南》，制定及檢視保安事故應變計劃；
5. 參考零信任及分隔網路段絡概念，以減低攻擊層面及受影響的網路範圍；
6. 備份所有重要資料，最少要有一份本地備份及異地備份；及
7. 加密所有敏感資料。

此外，HKCERT認為由於事故涉及個人資料外洩，有理由相信黑客將會或已經利用這些資料進行網絡釣魚攻擊及詐騙行為，建議公眾應加倍注意可疑電郵和來電，並採取以下保安建議：

1. 留意網址的英文串法，小心檢查有沒有錯誤或可疑之處，並且核實網站的真偽；
2. 切勿假設使用HTTPS 協定的網站是真實可信的，因釣魚網站亦可使用 HTTPS 協定；
3. 切勿隨意打開任何連結或附件，並於提供個人資料前三思；
4. 開啟電郵或者即時訊息內的附件或連結前，先確定發送者身份和內容；及
5. 定期為各帳戶更新登入密碼同啟用多重認證。

此外，大家若對電話號碼、電郵地址、網址和IP地址有懷疑，可以使用「守網者」的免費搜尋器「防騙視伏器」（https://cyberdefender.hk/scameter/）來核對是否詐騙和網絡陷阱。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/always-keep-system-security-up-to-date-to-prevent-customer-data-from-becoming-phishing-feeds

分析報告：分析間諜軟件 AgentTesla

根據以色列網絡安全方案供應商 Check Point 於11月上旬發表每月的《全球威脅指數》報告，名為「AgentTesla」的間諜軟件被列為全球最廣泛散布的惡意程式，影響逾 7% 企業。就此，HKCERT收集了其中一個AgentTesla惡意程式作樣本，以分析整個攻擊手法及背後運作，並提出保安建議，提升公眾的防禦能力。

什麼是 AgentTesla?

AgentTesla 是一個2014年出現並用 .Net 框架開發的間諜軟件，專門竊取用戶憑證。黑客可以使用這惡意軟件監視受害者，截取用戶於程式及瀏覽器中輸入的所有內容，然後把其傳輸至黑客控制的伺服器 (Command and Control Server)。

檢查電郵附件

黑客通常會透過釣魚郵件誘騙受害者下載一些惡意程式，在這個收集得到的樣本中，黑客便是以一個名為「PRE SHIPPING NOTICE.zip」的電郵附件企圖引導受害者下載開啟。

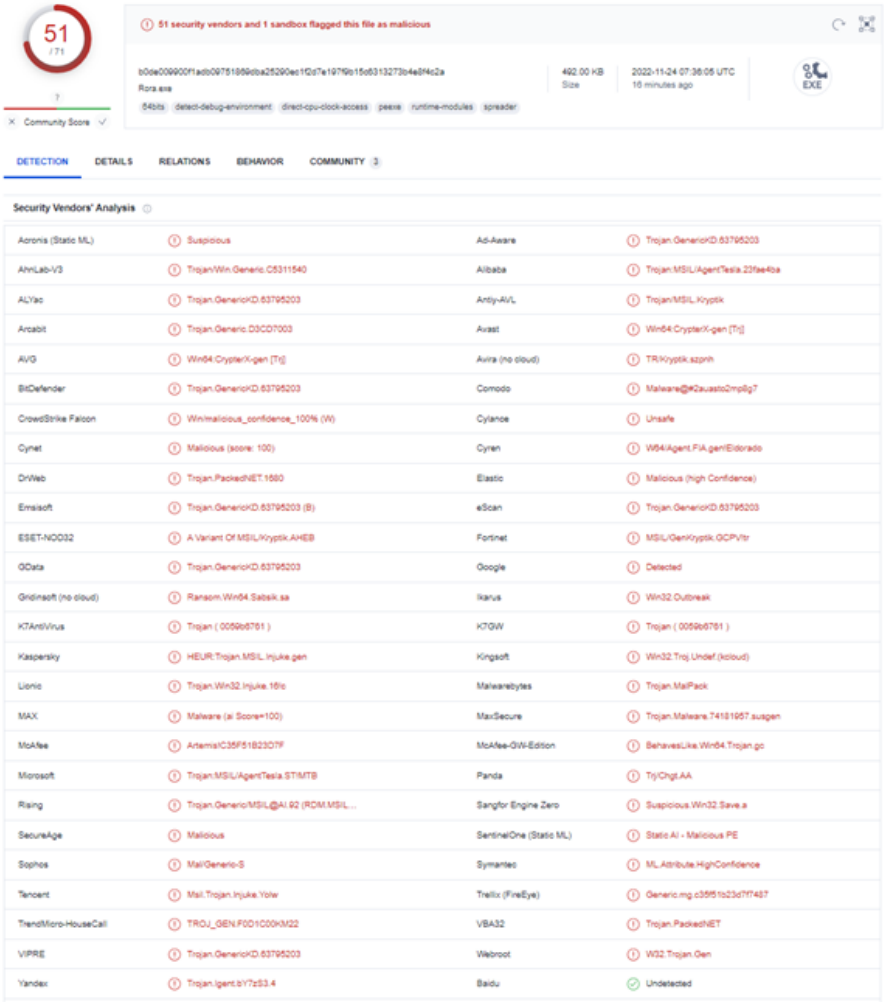
下載了「PRE SHIPPING NOTICE.zip」檔案後，通過解壓縮後得出一個名為「PRE SHIPPING NOTICE.exe」的檔案。

Name	Date modified	Type	Size
PRE SHIPPING NOTICE.exe	11/22/2022 8:35 AM	Application	492 KB

要放到 VirusTotal 上搜尋，可上載檔案的 SHA256 雜湊值，方法是用 Windows PowerShell 執行 Get-FileHash cmdlet 計算 SHA256 雜湊值(Hash value)，結果如下：

```
Algorithm       Hash
---------       ----
SHA256          B0DE009900F1ADB09751869DBA25290EC1F2D7E197F9B15C6313273B4E8F4C2A
```

然後，將這個雜湊值上傳至 VirusTotal 進行掃瞄，就已經有51間網絡保安公司能夠把它識別為惡意檔案，部份更能確認為 AgentTesla 間諜程式。



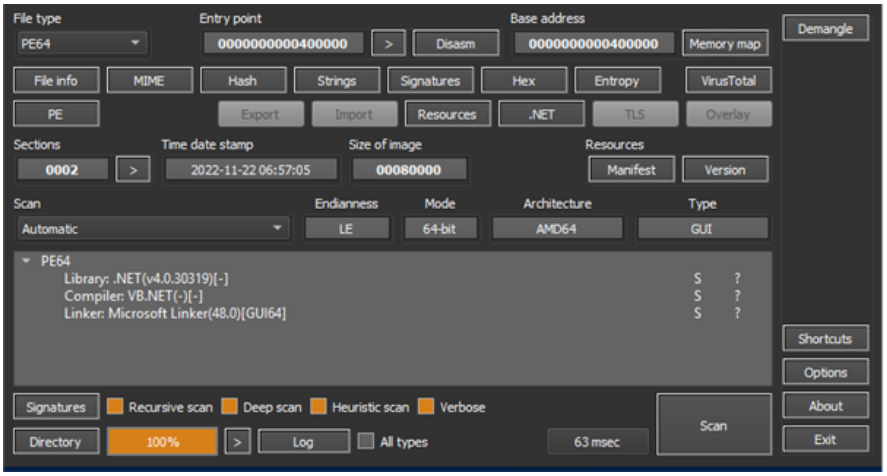
#搜尋於 2022 年 11 月 24 日進行

針對「PRE SHIPPING NOTICE.exe」進行分析

通過檔案鑑定工具對「PRE SHIPPING NOTICE.exe」進行分析，發現執行檔以 VB.NET 為編程語言，而且該檔案並沒有進行「加殼」(Packing)。

什麼是軟件「加殼」?

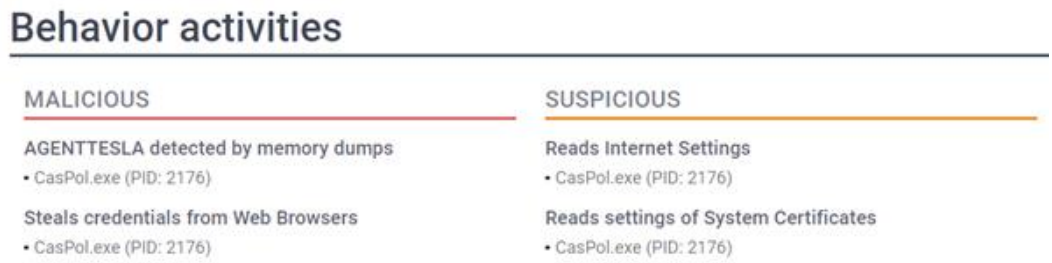
這是一種壓縮或加密可執行檔案的技術。加殼後會改變檔案的特徵碼，以試圖避免基於特徵碼掃瞄的防毒軟件檢測。



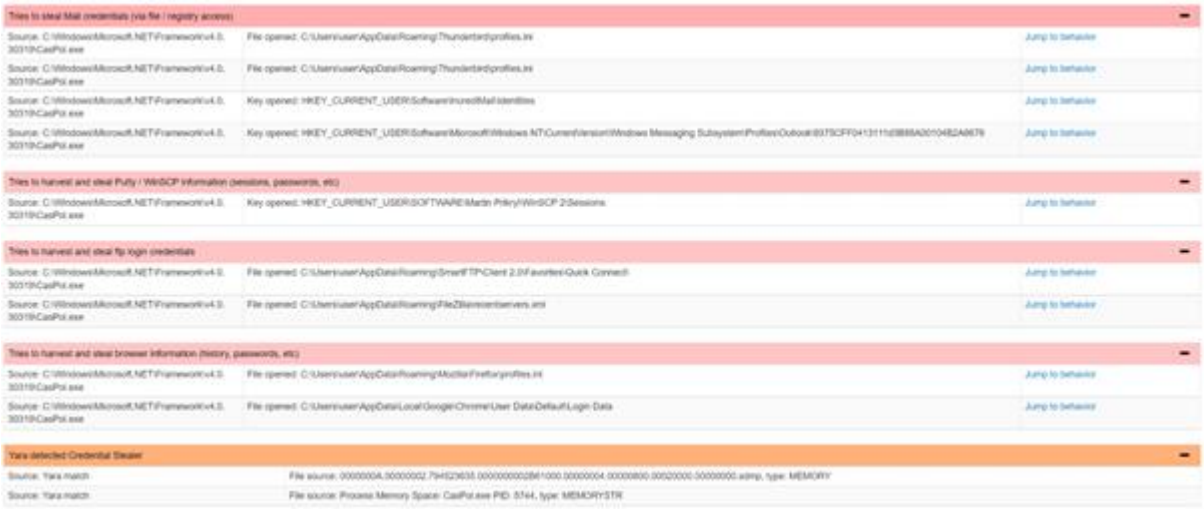
知道由哪個程式語言編寫後，便能方便進行逆向工程取得代碼。以下是通過對「PRE SHIPPING NOTICE.exe」而取得的其中一部分代碼，從代碼中可以看到 AgentTesla 會利用 Windows 的 ntdll.dll 寫入一些需要執行的負載（payload）。

```
private static void ConfuseSon()
{
  string St7rm = new string(">YeQ@yy".Select<char, char>((Func<char, char>) (c => (char) ((uint) c ^ 547U))).ToArray<char>());
  string B6th = new string("eYeQqz>rgdAAEo".Select<char, char>((Func<char, char>) (c => (char) ((uint) c ^ 547U))).ToArray<char>());
  IntPtr num1 = Ba77.Moni0or(Ba77.Fo1th(St7rm), B6th);
  uint C7v71;
  Ba77.Primari2y(num1, (uint) Ba77.\u0035ncreased.Length, 64U, out C7v71);
  uint num2;
  Ba77.Labe2(Process.GetCurrentProcess().Handle, num1, Ba77.\u0035ncreased, (uint) Ba77.\u0035ncreased.Length, out num2);
  Ba77.Primari2y(num1, (uint) Ba77.\u0035ncreased.Length, C7v71, out num2);
}

[DllImport("kernel32", EntryPoint = "GetProcAddress")]
private static extern IntPtr Moni0or(IntPtr 87for7, string B6th);

[DllImport("kernel32", EntryPoint = "LoadLibrary")]
private static extern IntPtr Fo1th(string St7rm);

[DllImport("kernel32.dll", EntryPoint = "VirtualProtect")]
private static extern bool Primari2y(
  IntPtr Ol1mpic,
  uint Cha22enge,
  uint Effec1,
  out uint C7v71);

[DllImport("ntdll.dll", EntryPoint = "NtWriteVirtualMemory", SetLastError = true)]
private static extern bool Labe2(
  IntPtr Ther3py,
  IntPtr T8ip,
  byte[] C7ke,
  uint Ma11ied,
  out uint O4d);
```

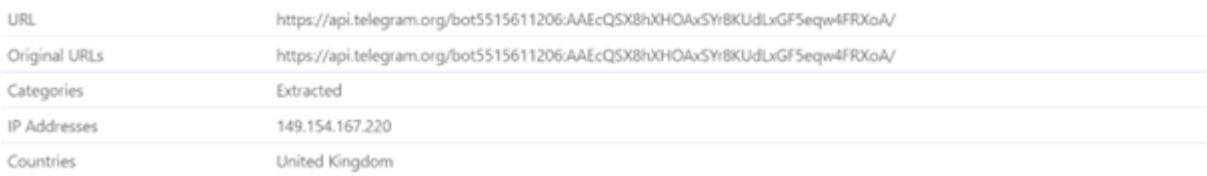
負載執行後，便偵測到 AgentTesla 會於受害者的電腦上所進行的惡意操作。它會偷取受害者電腦的設定、系統用戶憑證及瀏覽器內的憑證。



通過YARA惡意軟件研究及偵測工具可以更加容易顯示所偷取的資料，當中包括有不同的電郵設定檔(如thunderbird、incredimail、MS Outlook 等)、遠端伺服器的憑證(如 WinSCP、FileZilla)和瀏覽器所儲存的登入密碼(如 Firefox、Chrome 等)。



當完成偷取後，AgentTesla 會通過 Telegram API 將資料回傳至黑客的 Telegram 帳號。



保安建議

AgentTesla 的其中一個傳播途徑是以惡意電郵附件誘導用戶開啟，而網上更已出現多個變種版本，因此HKCERT 建議用戶：

1. 經常保持系統、軟件及防毒軟件於最更新狀態；
2. 切勿胡亂開啟不明檔案、網頁及電郵；
3. 開啟電郵內的附件及連結之前最好先確定寄件者身份及電郵內容；
4. 檢查文件的副檔名以免被檔案名稱誤導。不要開啟不明來歷的執行檔和 Microsoft Office 文件檔中的巨集：
    a. 執行檔的副檔名：.exe, .vbs, .js, .bat, msi, .ps, psc1, .cmd, .wsf, .jar, .reg等
    b. Microsoft Office 文件檔的巨集可以包含在所有類型的 Office 文件中（例如 .doc/.docm、.xls/.xlsm、.ppt/.pptm），建議用戶透過保安設定，禁止自動執行任何巨集
5. 用戶可以考慮使用密碼管理器來管理密碼，以取代將密碼儲存於瀏覽器；
6. 用戶應該使用較低權限的帳戶去處理日常工作，而非使用管理員帳號；及
7. 用戶可以設定「多重身份驗證」（MFA ）加強帳號保安。

詳細資料可參閱HKCERT保安博錄
https://www.hkcert.org/tc/blog/analysing-agenttesla-spyware

-完-

香港電腦保安事故協調中心
電話：8105 6060
電郵：hkcert@hkcert.org