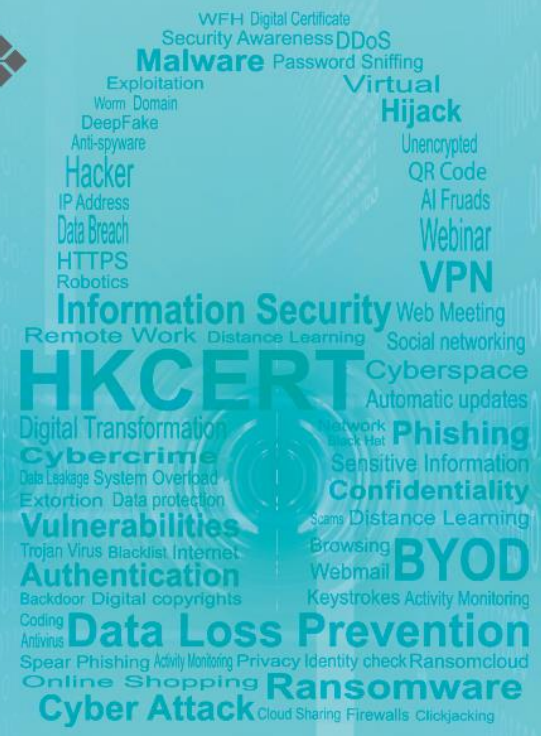
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2022 第三季度

發佈日期: 2022年11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、惡意程式寄存、殭屍網絡控制中心或殭屍電腦等)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(附錄1)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、惡意程式寄存	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
惡意程式寄存	CleanMX - Malware	2013-04
惡意程式寄存	Malc0de	2013-04
惡意程式寄存	MalwareDomainList	2013-04
殭屍電腦	Shadowserver - microso _sinkhole_events	2021-06

網絡攻擊類型	資料來源	開始使用
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	2022-10

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

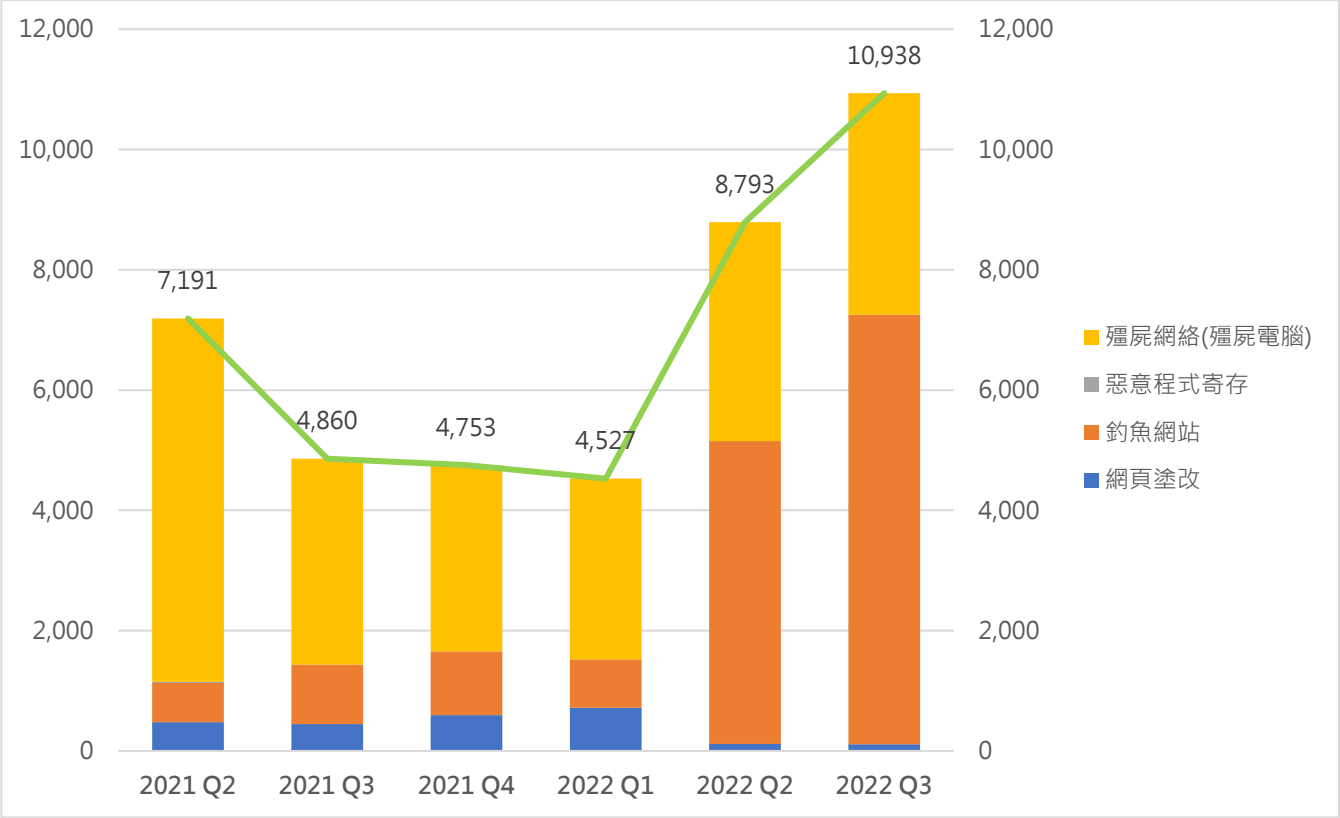
2022 第三季度報告概要

涉及香港的單一網絡保安事件宗數

10,938

按季上升

↑ 24%



事件類別	2021 Q3	2021 Q4	2022 Q1	2022 Q2	2022 Q3	按季
網頁塗改	445	595	718	118	113	-4%
釣魚網站	993	1,061	806	5,033	7,141	+42%
殭屍網絡(殭屍電腦)	3,422	3,097	3,003	3,642	3,684	+1%
總數	4,860	4,753	4,527	8,793	10,938	+24%

*相關數據來源沒有再提供殭屍網絡(控制中心)資訊。

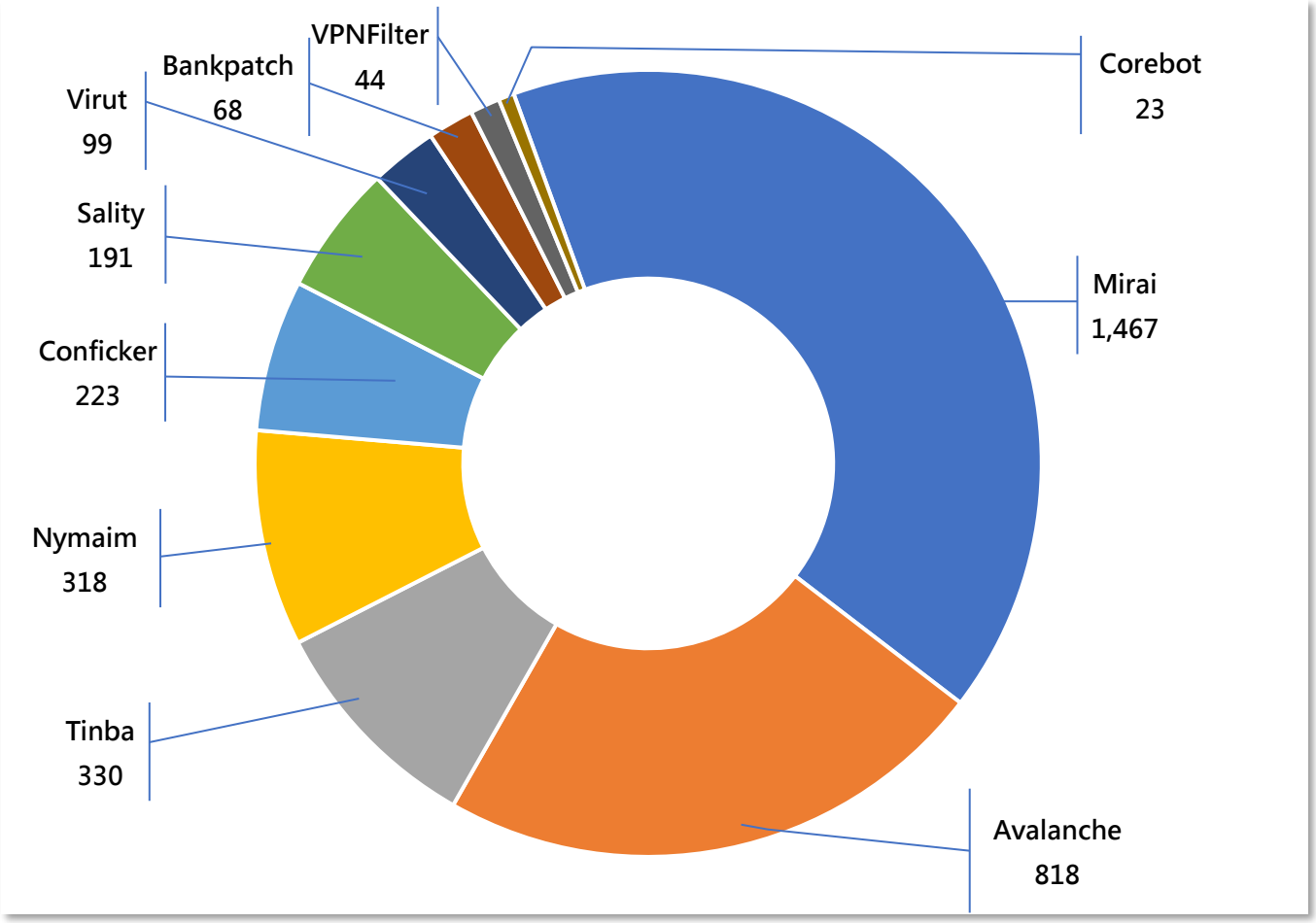
** 惡意程式寄存事件在對上五個季度皆為零宗。

香港網絡內的主要殭屍網絡

Mirai
1,467
↓ 5.1%

Avalanche
818
↑ 16.2%

Tinba	330	+42.2%
Nymaim	318	+43.2%
Conficker	223	-9.3%
Sality	191	-6.8%
Virut	99	-11.6%
Bankpatch	68	+88.9%
VPNFilter	44	-22.8%
Corebot	23	-42.5%



** 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。換而言之，由於不是所有殭屍電腦都一定在同一天開機，因此殭屍網絡的真實規模應該 比所見的數字更大。*

保安事件再次超越10,000宗

保安事件連升兩季，亦是自2020年第二季後首次再錄得過萬宗，與此同時，本地保安事件趨勢亦發生了變化，最明顯的是釣魚網站已代替殭屍網絡成為保安事件的主要來源。

在 2022 年第三季度檢測到的 7,000 多宗釣魚網站事件中，多達八成的網址擁有相似的結構，均是以一埋雜亂的字串，再加上`page1.php`作結尾，例如：`/k7OIMyJhEU/page1.php`、`/ic6oXx7P3s/page1.php`、`/uWBRvZ8quj/page1.php`或`/LAuCvx4R/page1.php`等。根據海外電郵保安專家的觀察，此類釣魚網站普遍以日文為主，內容是假冒信用咭公司或銀行，來騙取信用咭資料。黑客先發送電子郵件給用戶，以交易通知為藉口，再引導用戶點擊超連結前往需要輸入信用咭資料的釣魚網站。

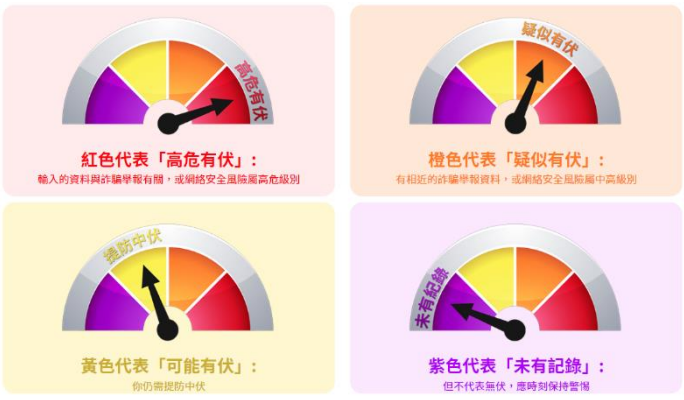
圖片：https://twitter.com/romonlyht/status/1566999640054333441

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。HKCERT呼籲用戶當遇到網站要求輸入敏感資料時，應立即提高警覺，謹記檢查清楚網址的英文串法以確定網站的真偽，如有懷疑，應立即離開網站及向有關機構查詢。

如何檢查網站安全可信?

除仔細檢視網址英文串法外，用戶亦可以使用由「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。它支援檢查電郵地址、網址和IP地址等，結果會以不同顏色警示：

> 搜尋結果亦會提供防騙提示，如交易或匯款前核實對方身分、提供敏感資料時保持審慎、切勿打開可疑連結或附件、留意+852字頭的本地來電等。



網絡安全小智識

電子郵件是其中一個網絡釣魚的主要攻擊途徑。當市民收到可疑電郵時，我們如何認清該電子郵件是否來自真正的發件人？除了辨認寄件者電郵地址外，每一封電郵中都會有一部份稱為「信件標頭」，當中包含電郵由哪個伺服器發出、發件日期、信息ID等等重要資訊。當中三項資料：寄件者原則架構 (SPF)、網域金鑰識別郵件(DKIM)及郵件驗證、報告和符合性(DMARC)，可以有助我們辨認電郵的真確性。從下列例子，三項資料結果為Pass。我們可判定該電子郵件是來自可信任及已獲授權的機構。

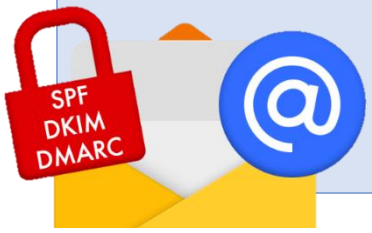
Headers Found

Header Name	Header Value
Authentication-Results	spf=pass ([redacted]) smtp.mailfrom=[redacted].com; dkim=pass ([redacted]) header.d=[redacted].com; dmarc=bestguesspass

什麼是SPF、DKIM 及 DMARC?

簡單來說，寄件者原則架構、網域金鑰識別郵件及郵件驗證、報告和符合性是處理電子郵件欺騙和網絡釣魚的一些技術，企業應審視電郵伺服器設定是否合適，避免公司電郵地址被盜用。

寄件者原則架構 (SPF)	指定獲得授權，可代表貴機構傳送電子郵件的伺服器和網域。 • 透過驗證SPF，收件者可以得知該郵件來自發件者的網域及是否同意發出這郵件。
網域金鑰識別郵件 (DKIM)	在每封外寄郵件中加入數位簽章，讓收件伺服器能確認郵件確實來自貴機構。 • 例如發件者在發出郵件時，會加入DKIM數位簽章（私鑰），藉此減少郵件被竄改的可能性。而收件者會透過檢查DKIM（公鑰），確保與原本加簽的私鑰一致。
郵件驗證、報告和符合性(DMARC)	如果機構寄出的郵件未通過 SPF 或 DKIM 驗證，你可以運用 DMARC 指示收件伺服器該如何處理這類郵件。 • 當SPF及DKIM驗證失敗時，DMARC可以幫助發件、隔離或拒收。可是，所發出的郵件通常會被標注為「垃圾郵件」。或者，如果DMARC設定為「拒絕」時，意味著不是從指定郵件服務器發出的郵件，便不能用該電郵地址發出。因此系統管理員應定時審視電子郵件系統的設定是否符合公司政策。



焦點：人工智能與網絡保安

近年，人工智能於企業的應用經歷了快速增長。根據國際數據資訊有限公司預測，世界各地的企業計劃在 2022年投放於人工智能方案（例如硬件、軟件、服務等）的支出將會增加19.6%，達4,328億美元，到2023年更會超過5,000億美元。隨著人工智能的應用變得多樣化，大家必須更加關注其相關的安全風險。否則，最終可能弊多於利。

什麼是人工智能？

人工智能，普遍指通過電腦程式呈現人類智能的技術，這些人類智能包括學習、解難和辨識規律等。目前人工智能技術正處於蓬勃發展階段，如電腦性能、機械人學和統計學提升，以及不斷增加的數據量。人工智能的應用日益廣泛，從廣為人知的電腦視覺（如圖像識別和人面辨識）及語言處理（如翻譯和語音辨識），逐漸拓展至模仿人類認知，如癌症判斷，甚至法律案件分析，作詩繪畫等。網絡安全方面，人工智能可用作辨識惡意程式。

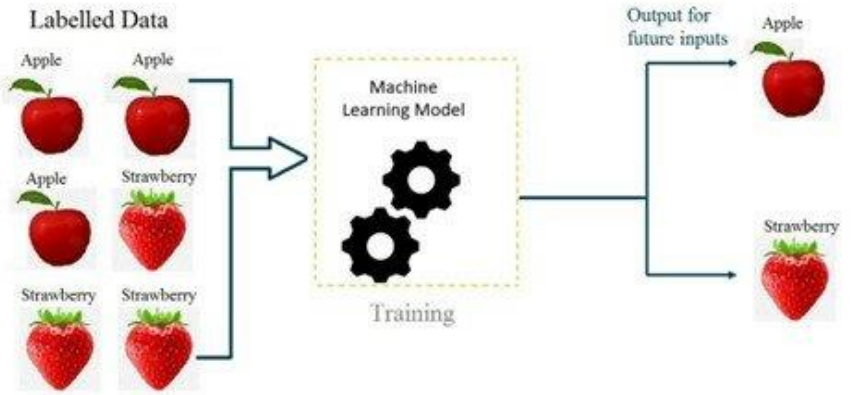
監督學習

機器學習的方法眾多，其中最常見的是監督學習。

- **基本原理**

  監督學習下，收集數據集以訓練一個數學模型，數據集內的數據包含一個或多個的輸入（或稱特徵）及輸出（或稱標籤），將這些特徵和標籤放入一些算式，計算出演算法用來預測輸出。

圖一：機器學習的基本原理，蘋果和士多啤梨影像及其特徵被稱為特徵，所表達的物件則為標籤



圖片來源：https://ai.plainenglish.io/introduction-to-machine-learning-2316e048ade3

人工智能系統之網絡保安風險

首先，如上文所述，人工智能建基於大量數據和計算，若這些數據中包含敏感資料，一旦洩漏便會導致敏感資料被披露。其次，收集的數據之收集可能來自多個來源，當中亦有交叉洩露的危險。第三，若受惡意攻擊，影響範圍更廣。如多個服務使用同一模型，當模型受到攻擊篡改，則所有使用該模型的服務皆會受到波及。無論你是人工智能的使用者與否，人工智能所帶來的網絡保安風險都可能影響你。在此以「保安漏洞」和「濫用」兩方面，討論人工智能對不同人士帶來的影響。

保安漏洞

- **成員推斷攻擊**

  是對機器學習模型（下稱目標模型）的輸出進行逆向工程 (Reverse Engineering)，從而推斷出用作訓練目標模型的數據。此攻擊的原理是因目標模型對已見和未見的輸入有不同的表現，如置信度 (Confidence Level)，故只需觀察模型的輸出，便有可能推斷某一輸入數據是否在訓練數據集內。

- **對抗性干擾**

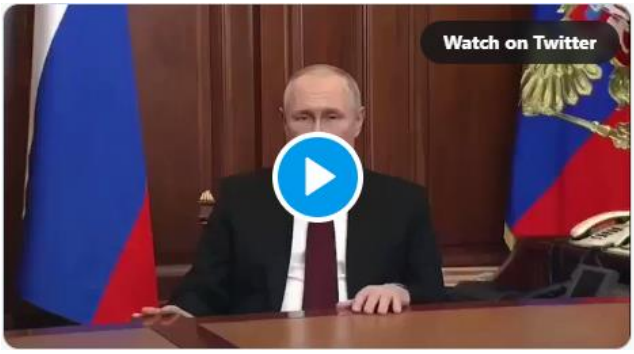
  是指刻意提供錯誤數據以干擾機械學習模型之判斷。其基本原理為透過對數據作微小更動，增加目標模型之誤差。當中又有閃避攻擊及中毒襲擊兩種。

人工智能的濫用 - 深度偽造 (深偽，Deepfake)

深度偽造是深度學習 (Deep Learning) 和偽造的混成詞。泛指以人工智能製作偽造訊息，如影像和聲音。常見於影片，影片中的人臉將被換成另一人面。這種技術亦可被用於偽造人聲，只需輸入字句便能假借受害者之聲線讀出，意味著製作深偽影片毋須有配音員。

深偽技術現在更發展到可將語音和影片中人的嘴唇同步。深偽的主要學習演算法有自編碼器 (Autoencoder) 和生成對抗網絡 (Generative Adversarial Network)。

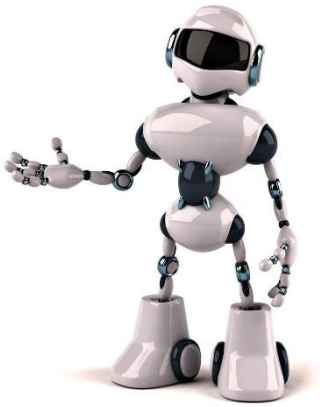
例如在 2022 俄羅斯烏克蘭戰爭中，兩國總統澤連斯基及普京的肖像亦被用作製造深偽影片以傳播謠言。



資料來源：https://www.youtube.com/watch?v=X17yrEV5sl4、https://twitter.com/sternenko/status/1504090918994993160?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504090918994993160%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Farticle%2Ffactcheck-putin-address-idUSL2N2VK1CC

保安建議

- 選擇適合的模型，以避免成員推斷攻擊
- 更新學習模型前驗證數據，以避免對抗性干擾
- 改善特權存取管理(PAM)制度
- 使用防偽工具避免深度偽造
- 加強對深偽的認知



總結

隨著人工智能的能力提升，人工智能亦被用作武器，今時今日，無論你是人工智能的使用者與否，都有機會成為這些攻擊的受害者。了解人工智能衍生的網絡保安風險，便能安心享受人工智能帶來的便利。

詳細資料可參閱竹HKCERT保安博錄
https://www.hkcert.org/tc/blog/adopt-good-cyber-security-practices-to-make-ai-your-friends-not-foes

分析報告：瀏覽器的反釣魚網站功能如何阻擋釣魚攻擊

過去四年HKCERT平均每年處理約8,900宗本地的網絡保安事故，當中在2021年釣魚攻擊更佔所有事故總數的48%，即使綜觀全球，釣魚攻擊亦佔保安事故總數的36%

釣魚攻擊數量繁多的原因？

釣魚攻擊是一種成本低但卻非常有效的攻擊，而且變化多端，現今技術可讓黑客容易建立仿真度高的假電郵及網站騙取用戶。 除直接騙取用戶的個人敏感資料外，如成功得到機構的系統（如VPN或SaaS）登入帳戶，更可繼而嘗試取得系統內的敏感資料或進行橫向移動 （意指攻擊者從入口點移動至網絡其餘部份的過程），入侵其他內部系統。

用戶如何防範釣魚網站

除了加強用戶的安全意識 (例如分辨可疑電郵及網址, 積極主動匯報可疑網址)外，一般防毒軟件及瀏覽器都會提供反釣魚網站功能，助用戶及機構減少存取可疑網站。

反釣魚網站功能及引擎

瀏覽器是連接網站的橋樑，其分辨釣魚網址的功能，亦是其中一個重要的防禦機制。常用的瀏覽器都附有反釣魚網站功能，當瀏覽器嘗試存取網頁時，反釣魚網站引擎會先將網址

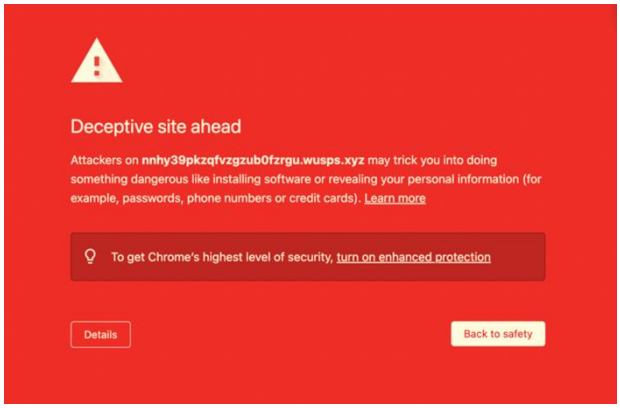
及釣魚網站數據庫內的資料進行比對及分析，如分析結果顯示為安全的話，用戶可以正常存取該網頁。相反，若分析結果顯示為不安全，則會彈出警告頁面以防用戶瀏覽。

因此，數據庫內的資料完整性及更新速度，對瀏覽器分辨釣魚網站有著重大影響。部份瀏覽器開發商會採用由其他開發商所建立的反釣魚網站引擎服務，以下是常用瀏覽器的比較：

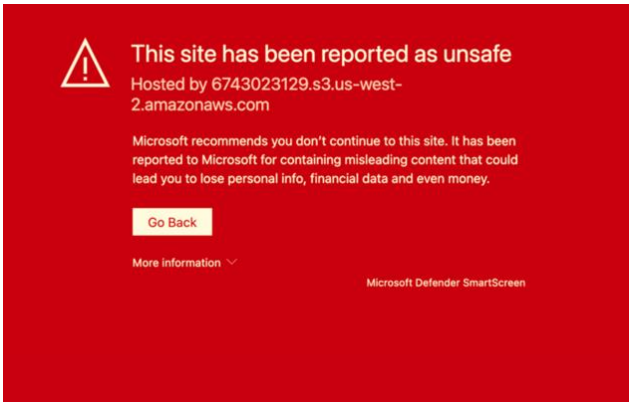
	Chrome	Edge	Safari	Brave	Firefox
反釣魚功能	有	有	有	有	有
反釣魚引擎	Google Safe Browsing	Microsoft Defender SmartScreen	Google Safe Browsing	Google Safe Browsing	Google Safe Browsing

由上表可見反釣魚網站引擎主要分為2個陣營：Google Safe Browsing和Microsoft Defender SmartScreen。以下是當這2款引擎判斷到釣魚網站時所顯示的警告樣板。

Google Safe Browsing



Microsoft Defender SmartScreen



近年釣魚攻擊趨勢

釣魚攻擊手法一直在演變，最近甚至利用人工智能客戶服務套取用戶提供敏感資料。有見及此，HKCERT分析及測試了本地用戶常用的瀏覽器，看看眾多瀏覽器的反釣魚網站效能。

測試目的

目的是針對一般用戶在瀏覽器預設保安設定情況下進行測試，記錄不同瀏覽器在桌面電腦及智能電話中對新近發現的釣魚網址的封阻效能。

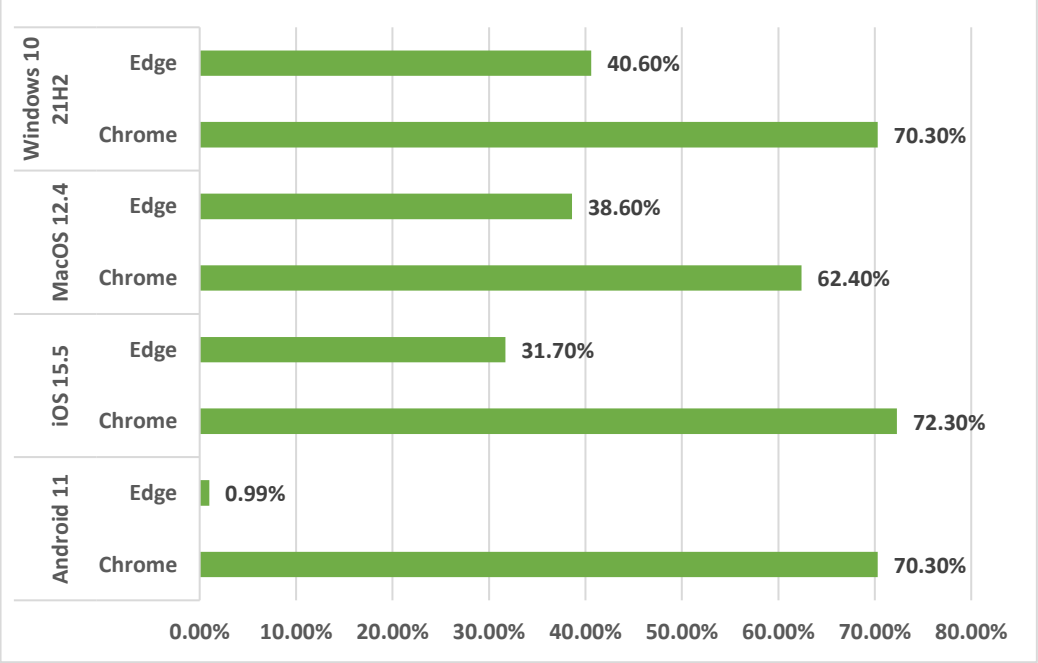
測試方法

由七月十一日至七月廿八日，每天從OpenPhish抽樣存取當日發佈的最新釣魚網址。

測試環境及瀏覽器

由於常用的瀏覽器所使用的反釣魚網站引擎主要分為2款，所以會在每款引擎中選取其中一個瀏覽器，於桌面及智能電話平台上進行測試。為模擬普遍用戶的真實使用情況，所有測試的瀏覽器均是使用預設的保安設定，測試結果以作為第一層防禦的瀏覽器能否封阻釣魚網站為準。

測試結果



1. 測試結果顯示 Chrome 在所有平台中封阻釣魚網頁的成功率都較 Edge 為高。
2. 相同瀏覽器於測試的作業系統中有不同表現，原因或與軟件商如何實行反釣魚網站引擎有關。
3. Edge 的反釣魚網站功能在 Android 中辨別率最低。HKCERT 就此曾查詢 Microsoft，獲回覆表示問題會於往後推出的新 SDK 版本中得到解決。 Microsoft 又指 HKCERT 的測試是基於 Microsoft Defender Smartscreen 的預設設定，如使用 Microsoft 的建議設定，測試結果可能不同，並建議用戶如有任何查詢，可與它們聯絡。

建議及總結

HKCERT 建議 Chrome 用戶啟用瀏覽器內的 Enhanced Protection 以提高攔截釣魚網頁的成功率。另外，由於瀏覽器的反釣魚網站功能需要時間收集及分析釣魚網址，所以瀏覽器對新註冊的釣魚網站的辨別率會相對較低。HKCERT 提醒用戶：

- 留意網址的英文串法，小心檢查有否錯誤或可疑之處，並核實該網站真偽；
- 切勿假設使用 HTTPS 協定的網站必是真實可信網站，釣魚網站亦可使用 HTTPS 協定；
- 不要隨意打開任何連結或附件，並於提供個人資料前三思；
- 不要透過電子郵件提供的連結或未知網站來登入帳號，可善用瀏覽器的書籤功能來儲存任何帳號登入的網址。

總而言之，反釣魚網站功能只能減少用戶存取釣魚網頁的機會，增強自身安全意識配合反釣魚網站功能才是對抗釣魚攻擊的上策。在現實中作一個例子，反釣魚網站功能像口罩，可以隔絕大部份病毒入侵，但當病毒通過口罩後，最終都是要靠自身的抵抗力去保護免受病毒入侵。

詳細資料可參閱竹HKCERT保安博錄
https://www.hkcert.org/tc/blog/browser-s-anti-phishing-feature-what-is-it-and-how-it-helps-to-block-phishing-attack

保安：繞過多重認證保護，盜用電郵帳號

最近Microsoft研究人員發現了一個大規模網絡釣魚活動，即使用戶啟用了多重認證 (multi-factor authentication, MFA) 也能被竊取電子郵箱帳號。研究表示這種手法的釣魚攻擊自 2021 年 9 月以來一直活躍，到今天為止已經試圖攻擊至少一萬個組織。

使用的技術其實不太難理解，這種技術名為中間人攻擊

1. 黑客部署代理伺服器及假網站，之後會對目標用戶發送釣魚郵件；
2. 用戶不虞有詐打開郵件中的假網站連結或者附件；
3. 用戶被重新定向去假網站，而假網站會要求用戶輸入電子郵箱帳號和密碼登入；
4. 用戶輸入帳號密碼並用MFA通過身份驗證，黑客建立的代理伺服器會將用戶輸入的資料重新導向到合法的網站頁面，從而使用戶成功登入；
5. 黑客則已經在後台截取了用戶憑據和身份驗證的資料，結果在用戶未發現的情況下，被黑客成功入侵用戶的電子郵箱帳號；

成功入侵後，黑客會查找用戶郵箱與付款或發票等相關的電郵會話，之後會假扮用戶發出欺詐郵件，例如要求用戶的客人或者同事向黑客銀行帳戶匯款。

為了讓受害用戶注意不了可疑的郵件會話，黑客更會刪除他們發出的欺詐電郵，同時建立收件箱規則去隱藏欺詐目標回覆的電郵。例如設定用戶郵箱收到被欺詐目標的電郵時，該電郵會自動刪除或移動到archive文件夾並將其標記為已讀。

縱使這類攻擊手法能夠繞過 MFA，但無可否認 MFA 在阻止其他各種攻擊方式仍然非常有效，因此用戶最好還是使用 MFA 來保護帳號安全。

保安建議

- 輸入任何登入資訊前，檢查登入頁面的網址以確保連接到官方登入網站
- 不要打開可疑的電子郵件或信息
- 不要打開任何不明電郵中的網站連結或附件
- 不要透過電子郵件提供的連結或未知網站來登入帳號
- 檢查收件箱設置是否異常，例如可疑的收件箱規則或賬戶活動記錄
- 使用更高規格的認證技術，例如硬件FIDO (Fast IDentity Online) 免密碼登入認證

-完-

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