一、　摘要

美國國土安全部（DHS）網絡安全和基礎設施安全局（CISA）和英國國家網絡安全中心（NCSC）聯合針對：用目前 COVID-19(武漢肺炎) 網絡犯罪和進階持續威脅性組織（APT），進行網路攻擊提出警訊。

CISA 和 NCSC 注意到：駭客組織開始利用與 COVID-19 為主題的網路攻擊；同時，遠距辦公使得易受攻擊網路服務（如 VPN）的使用，加劇了對個人和組織的資安威脅。這些進階持續威脅性組織和網絡犯罪針對個人，中小企業和大型組織，利用 COVID-19 的相關主題，進行網路詐騙和釣魚電子郵件。本警訊解釋這些與 COVID-19 相關的惡意活動，並提供了一些個人和組織能遵循的實用建議，以減少受影響的風險。

由於攻擊的情況快速發展，該警訊未對所有的 COVID-19 相關惡意活動進行分類，個人和組織應採取積極性的措施來自我防護。

二、　技術性細節

（一）　攻擊手法摘要

這些進階持續威脅性組織開始利用 COVID-19 疫情的大流行作為其主要攻擊手法的一部分，惡意人士通常會偽裝成可信任的單位，有時會偽裝成先前已被攻擊的單位，傳送以 COVID-19 為主題的釣魚訊息或惡意程式，犯罪者利用疫情來獲取商業利益並散布各種的勒索病毒和惡意軟體，以達到間諜活動、駭客活動、資訊竊取的長期目標。

接下來的數周或數月，進階持續威脅性組織可能繼續利用 COVID-19 的大流行來從事活動。目前已觀察到的活動包括：

- 以 COVID-19 為誘餌的網路釣魚；
- 以 COVID-19 為誘餌的惡意軟體；
- 以 COVID-19 組成的網域名稱註冊；
- 針對遠端存取、遠端控制或遠端辦公基礎設施的攻擊。

惡意人士利用社交工程手法來誘導使用者進行特定操作，利用人性的弱點（例如好奇心和對疫情的恐懼）來誘使受害者從事以下操作：

- 開啟釣魚網站連結或下載內含釣魚連結的應用程式，或下載夾帶勒索軟體的惡意程式。例如：一個 Android 應用程式偽裝成疫情的最新資訊，試圖誘導使用者授權設備存取，以安裝名為「CovidLock」的勒索軟體。

- 開啟內含惡意軟體的檔案（附件）。例如以 COVID-19 為主題的內容，如：「武漢肺炎最新資訊」、「所在城市的最新疫情」、「緊急狀態」等。

為了營造真實感，惡意人士會在電子郵件中偽造發信者的資訊，讓其看上去是來自從可信賴的來源，例如「世界衛生組織（WHO）」或「譚德賽」。在幾個案例中，惡意人士發送釣魚郵件，並包含偽冒的登入頁面，其他的案例包含偽裝人資部門並要求員工開啟郵件附件。這些附件可能以武漢肺炎或 COVID-19 為檔名，例如「總統與內閣通過由於武漢肺炎導致的預算刪減」。

（二） 網路釣魚

CISA 和 NCSC 皆觀察到大量利用上述社交工程技術的網路釣魚活動。其所使用的主旨包括：

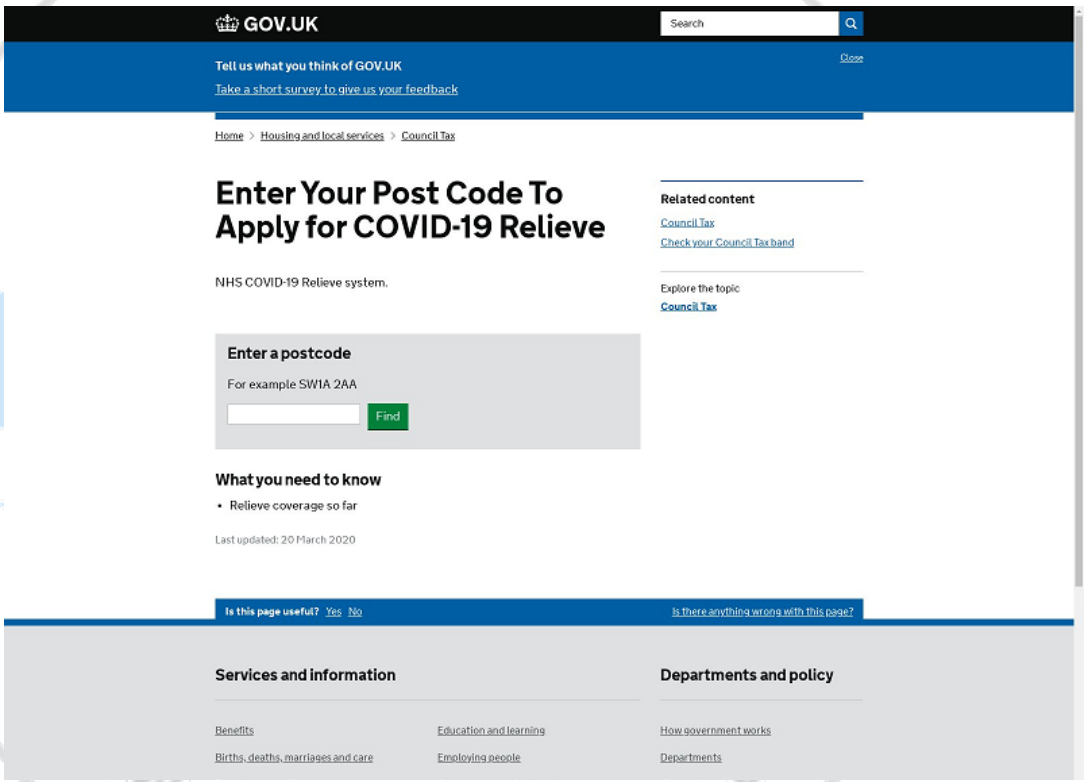
- 2020 冠狀病毒最新資訊；
- 冠狀病毒最新資訊；
- 2019-nCov：所在城市的最新確診病例；
- 2019-nCov：所在城市疫情爆發（緊急）。

這些電子郵件可能要求從事行動，鼓勵受害者開啟惡意人士所架設的網站並提供有價值的資料（如使用者名稱和密碼、信用卡資訊和其他個人資料）。

（三） 簡訊釣魚

儘管大多數的網路釣魚皆透過電子郵件，NCSC 以察覺到一些嘗試其他手段來進行（例如手機簡訊）來進行的網路釣魚。

從前，這些釣魚簡訊通常使用財務上的誘因（例如政府補助或退稅）來做為誘餌。COVID-19 相關的釣魚活動則延伸自財務上的內容，特別是流行性疾病對財務的影響，以及政府在就業或經濟上的支援計畫。例如：有一系列的簡訊偽裝成英國政府，藉此收集關於電子郵件、地址、姓名、銀行帳戶等資訊，這些簡訊號稱來自 UKGOV 或與 COVID 相關，並包含了釣魚網站的連結。



如同上述示例，惡意訊息可能透過電子郵件以外的方式散布，除了簡訊，可能的方式包含 WhatsApp 和其他通訊服務。惡意人士可能繼續示財務相關內容來從事釣魚活動，具體而言，政府的新措施可能成為新的釣魚手段。

（四） 利用釣魚竊取登入資訊

許多惡意人士使用與 COVID-19 相關的網路釣魚來竊取使用者的登入資訊，這些電子郵件透過上述的社交工程手段，有時並輔與緊急用語來增加說服力。

如果使用者開啟網站，便會顯示一個包含密碼輸入欄位的詐欺網站，其可能與各種線上服務相關，包含 Google 和微軟的電子郵件服務，或是政府服務的登入頁面。

為了更進一步說服受害者，這些網站通常在網址中會包含與 COVID-19 相關的措辭，例如「corona-virus-business-update」、「covid19-advisory」、「cov19esupport」等，這些偽冒的網址使其看起來合法或類似知名網站，辨識惡意偽冒網站的唯一方法是檢查網站的網址。在某些情況下，惡意人士會根據受害者來修飾這些偽冒的登入頁面。

倘若受害者在這些偽冒的頁面上輸入個人密碼或登入資訊，攻擊者便能存取受害者的網路帳戶，例如電子郵件，並獲得權限來存取個人的敏感資訊，或使用受害者的通訊錄來進一步散布釣魚郵件。

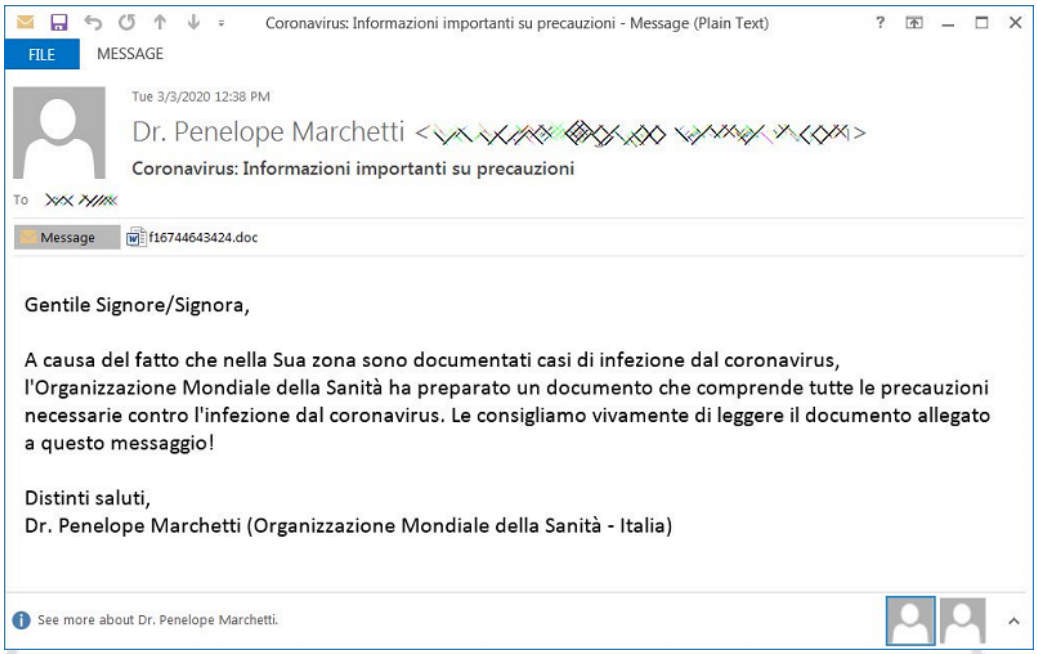
（五） 利用網路釣魚散布惡意程式

許多惡意人士使用 COVID-19 相關網路釣魚散布惡意程式。大多數的情況下，惡意人士會傳送電子郵件，誘導受害者開啟附件或從網站連結下載檔案。當受害者打開連結時，將執行惡意程式，從而危害使用者設備。

NCSC 發現一個名為「Agent Tesla」的鍵盤輸入記錄程式，透過各種不同的電子郵件散布。該電子郵件偽冒世界衛生組織秘書長譚得賽・阿德諾姆・格布瑞索斯博士的名義傳送，這個電子郵件的惡意活動開始於 2020 年 3 月 19 日。另一個類似的案例宣稱將提供溫度計和口罩以防範疫情，該郵件宣稱附加這些用品的圖片，但實則夾帶了「Agent Tesla」惡意程式。

在其他案例中，郵件會包含 Excel 試算表附件，或包含網頁頁面連結下載試算表檔案，在這兩種情況底下，該試算表中皆包含巨集程式，如果使用者啟動了巨集，將執行嵌入式動態鏈接庫（DLL）並安裝「Get2 loader」惡意程式。「Get2 loader」已被發現內含「GraceWire」木馬程式。

另一個被稱為「TrickBot」的惡意程式也被發現。在一個案例中，一封針對義大利使用者的電子郵件宣稱為 COVID-19 的相關訊息，其附件檔案帶有一個內含惡意程序的巨集，一但巨集執行，JavaScript 將被啟動並在系統中執行名為「TrickBot」的惡意檔案。



在許多案例中，木馬程式（如 Trickbot 和 GraceWire）將下載其他惡意檔案，如遠端存取的木馬程式或桌面分享軟體、勒索軟體。為了最大化的提升受害者付款可能，犯罪人士通常會在一個機構承受更大壓力時實施攻擊，在美國、西班牙和歐洲各地都有醫院或衛生組織收到勒索軟體影響。

個人和機構都應注意這些持續發展的釣魚活動，CISA 和 NCSC 都提供了能緩解惡意軟體和勒索軟體攻擊的指導方針。

（六） 危害遠距辦公的設備

許多組織已快速的建立了新的網路，包含 VPN 和相關的 IT 基礎設施。惡意人士會利用 VPN 和其他遠距辦公軟體中已知的漏洞。

在案例中，CISA 和 NCSC 發現有惡意人士掃描 Citrix 系統的已知漏洞，自 2020 年 1 月開始，CVE-2019-19781 已經被大範圍報導，CISA 和 NCSC 都提供了該漏洞的指導方針，並將繼續調查此漏洞。

已知的漏洞也影響許多 VPN 產品，如 Pulse Secure、Fortinet 和 Palo Alto。CISA 提供有關 Pulse Secure 漏洞的指導方針，而 NCSC 提供有關 Pulse Secure、Fortinet、Palo Alto 中的漏洞指南。

惡意人士嘗試利用使用量爆增的通訊平台，如 Zoom 和微軟 Teams，透過釣魚電子郵件，並夾帶如「zoom-us-zoom _ ##########.exe」、「microsoft-teams_V#mu#D_##########.exe」的惡意檔案，CISA 和 NCSC 也發現到知名通訊平台網站的仿冒。此外，攻擊者也能劫持未建立安全措示（如密碼保護）或舊版未更新軟體的線上會議或線上課程。

遠距辦公的興起也到導致了微軟遠端桌面連線（RDP）的使用量增加，對於不安全的 RDP 終端從事的攻擊活動已被大量回報，近期的分析報告了不安全的 RDP 終端增加了 127%，RDP 使用的增加可能使未建立適當安全措施的 IT 系統更容易遭受攻擊。

三、　緩解措施

（一）針對個人的網路釣魚指導方針

NCSC 提供了幾個主要的技巧來辨識網路釣魚電子郵件：

- 權威性：寄件人是否宣稱為官方人士（例如銀行、醫院、律師或政府機關），犯罪者通常會假裝是重要人物或組織來誘導受害者從事特定行為。
- 急迫性：其是否告知回復的期限有限（要求 24 小時或立即回覆），犯罪者通常以罰款或其他負面的後果來威脅受害者。
- 情緒性：訊息是否令人恐慌、害怕、希望或好奇，惡意人士經常使用具威脅性的語言，尋求支持或嘗試令受害者主動了解更多。
- 稀有性：該訊息是否提供一些稀有的資源（如演唱會門票、錢財、醫療用品），害怕錯過一個好的交易或機會可能令受害者更快的回應。

（二）針對組織或網路安全專業人士的網路釣魚指導方針

組織對網絡釣魚的防禦通常取決於使用者是否能夠發現網絡釣魚電子郵件。但是，能擴大防禦範圍並採用更多技術措施的組織可以提升對於網路釣魚攻擊的抵禦能力。

除了對於使用者的教育訓練，組織亦應考慮 NCSC 的指導方針。該指導方針將措施分為四個階層，在階層上建立防禦措施：

1. 令攻擊者更難接觸使用者
2. 幫助使用者辨識並通報可疑的網路釣魚電子郵件
3. 保護組織以避免受到未偵測到之釣魚郵件影響
4. 快速處理事件

CISA 和 NCSC 也建議有時可以讓組織中部份的釣魚攻擊成功執行，這能幫助最小化事件的損害。

（三） 針對組織或個人使用通訊平台的指導方針

由於 COVID-19 疫情，越來越多的私人或組織開始使用通訊平台（例如 Zoom 和微軟 Teams）進行線上會議，惡意人士也在入侵未受密碼保護或未安裝修復的軟體和會議。

避免線上會議受到劫持的技巧：

- 不進行公開會議，要求輸入會議密碼或使用等候功能並控制使用者的進入。
- 不要在未受限制的公開社交媒體分享會議連結，應直接向特定人員提供會議連結。
- 管理螢幕分享選項。將螢幕分享更改為「僅限主機」。
- 確保使用的遠距軟體的最新版本。
- 確保遠距辦公政策滿足實體和資訊安全要求

四、 版權聲明