2023
第二季電子郵件安全觀察

ASRC

Spam Mail
Virus Mail
Malicious Mail

July 2023 released.

2023 第二季，整體垃圾郵件、釣魚郵件數量微幅上升，常見病毒附檔郵件有些許減少，來自新申請域名的垃圾郵件約較上季增加 60%。不確定是否因為生成式AI的出現，讓語言在郵件的隔閡明顯被打破：這些過去常用英語書寫的詐騙郵件，轉成中文內容時，變得比過去更加流利了；同樣的情況也發生在過去出現在非英語語系流行的詐騙郵件，英文的詐騙內容文法變得流利，更不容易看出破綻。另一個較特別的威脅郵件是簡體中文的釣魚郵件，數量較上一季飆升許多，濫發時間落在三月底四月初；巧合的是，奈及利亞詐騙也在這個時間區間有明顯的大量濫發。

本季特殊郵件攻擊樣本解析：

釣魚郵件搭配 QRcode 進行攻擊，手機成為新破口

第二季，我們觀察到大量而持續的簡體中文釣魚郵件大量寄發，攻擊時間持續了一整季。這波釣魚郵件的主要特色為冒用政府或公司公告郵件，假借補助、退款或其他名義，進行釣魚詐騙，並且不帶有任何文字內文；一般釣魚郵件常見的釣魚連結及誘騙受害者點擊的社交工程文字內文，則被攻擊者分別以 QRcode 及圖片格式的方式隱蔽，藉以躲開傳統的超連結及文字掃描。

以 QRcode 及圖片格式的方式隱蔽釣魚連結及社交工程文字

我們觀察了許多樣本，發現攻擊者除了試圖以 QRcode 及圖片格式妨礙掃描外，也試圖挑戰郵件掃描機制對圖片的解析功能，例如同一類型的攻擊，圖片夾帶的方式就有一般圖片附件、非圖片附件及透過 HTML 的 <img> tag將圖片內嵌於內文三種方式。

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">=0D=0A<HTML><=
HEAD>=0D=0A<META content=3D"text/html; charset=3Dutf-8" http-equiv=3DConten=
t-Type>=0D=0A<META name=3DGENERATOR content=3D"MSHTML 11.00.9600.18315"></H=
EAD>=0D=0A<BODY>=0D=0A<P><img src=3D"cid:_Foxmail.1@a6387981-3c20-49fa-ac38=
-b8738b385aba" style=3D"width:518px;height:703px; "id=3D"img_insert_9303830=
35058879127528605105300"></P></BODY></HTML>=0D=0A
--------=_002_NextPart451744533084_=----
Content-Type: application/octet-stream;
   name="MRUL9PZcXMus.yh02A"
Content-Transfer-Encoding: base64
Content-Disposition: inline
Content-ID: <_Foxmail.1@a6387981-3c20-49fa-ac38-b8738b385aba>
```


```
/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAA8KCw0LCQ8NDA0REA8RFiUYFhQUFi0gIhslNS84NzQv
NDM7QlVIOz9QPzM0SmRLUFdaX2BfOUdob2dcblVdX1v/2wBDARARERYTFisYGCtbPTQ9W1tbW1tb
W1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1tbW1v/wAARCAK/AgYDASIA
AhEBAxEB/8QAHwAAAQUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQA
AAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKSo0NTY3
ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWm
p6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+Tl5ufo6erx8vP09fb3+Pn6/8QAHwEA
AwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSEx
BhJBUQdhcRMiMoEIFEKRobHBCSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElK
U1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3
uLm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwD0Siii
gAooooAKKKKACiiigBG6U2nN0ptABRRRQAUUjMFUk9BWZfaisURdm8tB+ZrGrWjSu5cIObsjReV
E+8wFM+1Q/3v0rjbnW55Mm3j2oP42GTTLa+uJQWmvGUDjAAHPauV4mpukdywMlG8jtRdRH+MCpVZ
WGVINcCdTvY5NgmMmOzIK0tP1v8AeiO4BhfpkHimsVNayWgp4GUVdHW0VVt7reQj9exq1XXTqRqK
8ThlFxdmFFFH16VoSFFZMmqhdRXac2agrLKANoc9Ofzz9adfXlyt5bQ2hibzWyecnYByTxwPer5G
```


非圖片附件方式夾帶

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META content="text/html; charset=utf-8" http-equiv=Content-Type>
<META name=GENERATOR content="MSHTML 11.00.9600.18315"></HEAD>
<BODY>
<P><img src="
```


```
ZoPMUYHynFaFqt2C32p4mGPl2AilOSaQRWrOfneOSRZJr0yEdpYW259hS3EiXCrvnjXH3WW3YEfjWjLosstx5z3jEg5XcgOKdPpMtygWe
MQxFVDJLeQubaFHtVukkMkUTrubqxwScAUAben6zLqUO6GO1VypKxm5y+R6jb0qKfxDLZxW5uraKKSTh0eYhkPrtCk7eOtZ2jNJe3CTPJ
kk3BgAcDoM569qtKiQ6hYW63zTvExBiJT5AEPOAAfzoQM26KKKACiiigAooooAKKKACiiigAooooAKKKACiiigAooooAKKKACiiigA
qk2lzJJIkVtF+8iMW63hSJBkjJPzknGPSuhooArCSZbwxNFmFlyki9iOoP9KnclVyFLewp1FAGVqD3V1biNNOuARIj/M0fQMD/f8AarDT
LqMMs7+WfKZkEbswQqASe2evtQBo/2xpu8p9ut8gZz5gx+fSrCXETymNXBbaGx6g9x61yYukDmf7U2WUDibJxn2uN3fpV6K4ni1dU23CK
IVQMkk4Aqs2p2CMVe9tlYdQZVB/nQA0abCNhYu7K5kZnIJclSvP4HpTjYo0IhLyFFkV1y2SMEEDPpxTv7QswUH2uDMnKDzB8309amEqGQ
RxIiMfmQY54I/TFNgar6jbosTEyN5y7kCROxI45wBkdR1p0F7BOJCjMPK+/5iMhXjPRgO1c1CrRwWky2r5MMkjBXWDcPkyQYh09jzVy3Y
70YPy57kDsajGlwYiG+ceVEIl2ysmQPXaRVppokcK8iKx6AkAnnH86jmv7O3fZPdQRP12vIFP60AV49JihmklinuFd+AxfeV6ZxuB/ujr
2VkmXpL22icpJcRIw6hnANBvYPs8kySLIkYydhzWNf3csLmKKXyViUBQCMkEDrlufripLUm5tpIljV0R1LLGFy/c5yx9PXNLm6FexSipM
WnR6fK0TxTBArkEtkOeBjgbQBwK1aKXKi/ayM46RbCVXjUIoILKFHzY6c09rWXZcszq8kse0BV2gYzjufWr1FPlQnUk92Z0lvNcxrA6+X
Cb3/n5t//AB7/AAoA6D/hKdG/5/P/ACE/+FH/AA1Ojf8AP5/5Cf8Awrn/APhCb3/n5t//AB7/AAo/4Qm9/wCfm3/8e/woA6D/AISnRv8A
AkYrX/gf/AKA1ABrGgTaRDHLLNHIHbaAoNa/gL/l//wC2f/s1bWu6P/bNvHF5/k7G3Z2bs8fUVgsz+DZCiFbv7UoJJGzbtz7n1oA2dX8R
B/wB/U/xr0GaRYYXlf7qKWOPQCo7K5F5ZxXKqVEqhgD2p11EZ7WaIHBkRlz9RigDmdb8SaffaVcW0JkLuBjKYHUGuNroNR8Kz6fZS3T3M
AMjxZ/wAi7df8A/8AQ1rn/Av/ACErj/rj/wCzCug8Wf8AIu3X/AP/AENa5/wL/wAhK4/64/8AswoAs+Pf+XD/ALaf+y1yFdf49/5cP+2r
qtHExRmlM7x4LNt+783OQSTg9MCgDWfV9ORwrX1vknH+sHH19KU6naYUpL5wbODApl6Yz90H1FZdgl5I4/fyxhY48LEV+VWBOSGUgnj2p
D/aiCORpIJ42jVW8tgu5gTgEYOOvvVOx0zZo89ukCwSybxyuCeTjPJ4/E1P5UlxLJcXFizJ5Qj8hijF+ck9cfrQBYe+McStJbTrI77Ei+
```

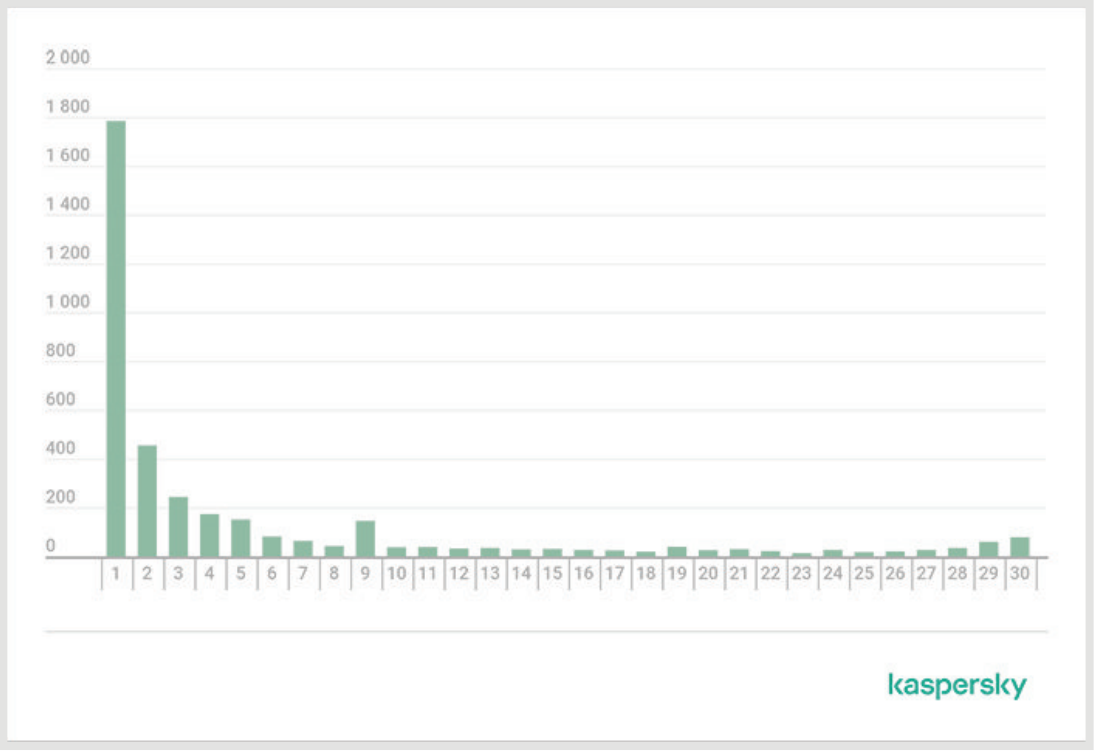

透過 HTML 的 <img> tag 將圖片內嵌於內文

這樣的手段除了可以嘗試突破郵件掃描機制外，攻擊者也可能藉由這些攻擊穿透成功的統計，推測郵件掃描機制對夾帶圖片的處理方式或實作上的弱點，用以改良後續的攻擊手段。

此外，由於惡意連結藏在 QRcode 中，所以慣於用手機掃描 QRcode 內容的受害者，曝險的對象由電腦轉向了手機，企業較多保護措施的終端對象通常是工作用電腦，而個人用的手機就成了新的風險突破口。

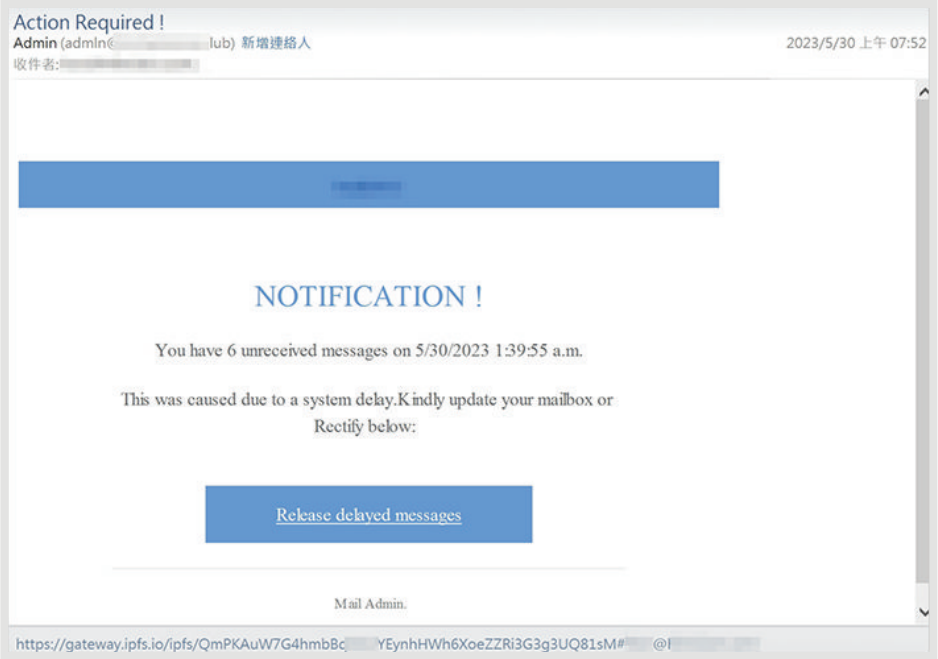
存活時間長，難以滅絕的釣魚網站

在過去，釣魚網站的生命週期都不長，尤其是寄宿在有管理的服務主機或域名上的釣魚網站。根據卡巴斯基公司在 2021 年揭露的釣魚網站活動統計，多數的釣魚網站在一天後，甚至是出現的數小時之後，就已經處於非活動 (inactive) 狀態。



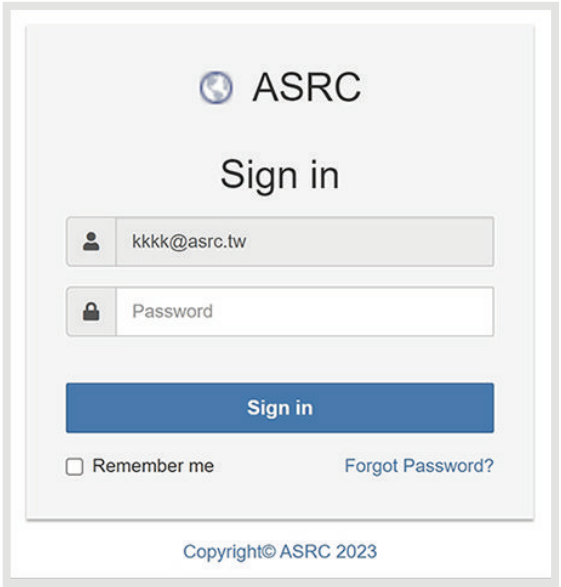
釣魚網站生命週期統計 (引用來源：https://securelist.com/phishing-page-life-cycle/105171/)

第二季開始，我們明顯觀察到有許多的釣魚郵件開始搭配星際檔案系統（InterPlanetary File System，縮寫為IPFS）作為釣魚網站。IPFS 是一個對等的分散式檔案系統，沒有採用傳統的集中式架構，而是使用遍布全球的點對點 (P2P) 數據網絡，無需第三方或中央機構管理，因此，IPFS 網絡釣魚內容可以很容易地分發，更難以檢測，並且具有持久性，這樣的釣魚網站只能由建立者自行刪除。



利用 IPFS 的釣魚郵件

以 IPFS 建構的釣魚網站，存活時間非常久，直至截稿前，這些惡意的釣魚網站仍在正常運行。並且這個釣魚網站會根據攻擊目標 E-Mail 帳號的域名進行頁面的標題變化，藉此降低戒心；當受害者第一次輸入密碼時，系統會回應密碼錯誤，再輸入第二次竊取密碼後，將頁面重新導向至目標 E-Mail 帳號的域名。



這個釣魚網站會根據攻擊目標 E-Mail 帳號的域名進行頁面的標題變化

結語

利用 IPFS 建設的釣魚網站，由於其分散系統的特性，沒有中央機構可以對它稽查或管理，再加上 IPFS 還可搭配縮址、轉址等功能進行更複雜的矇騙或躲避稽查，未來可能會變成釣魚網站存在的主流趨勢。

企業防禦最直接的方式是避免接觸這類的釣魚郵件，採用優良的郵件掃描機制是一個好方法；此外，在無必要使用 IPFS 的前提下，直接隔離 IPFS 網址，也可讓此類風險大幅度降低。

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 https://www.asrc-global.com/

ASRC垃圾訊息研究中心