2023
第三季電子郵件安全觀察

ASRC

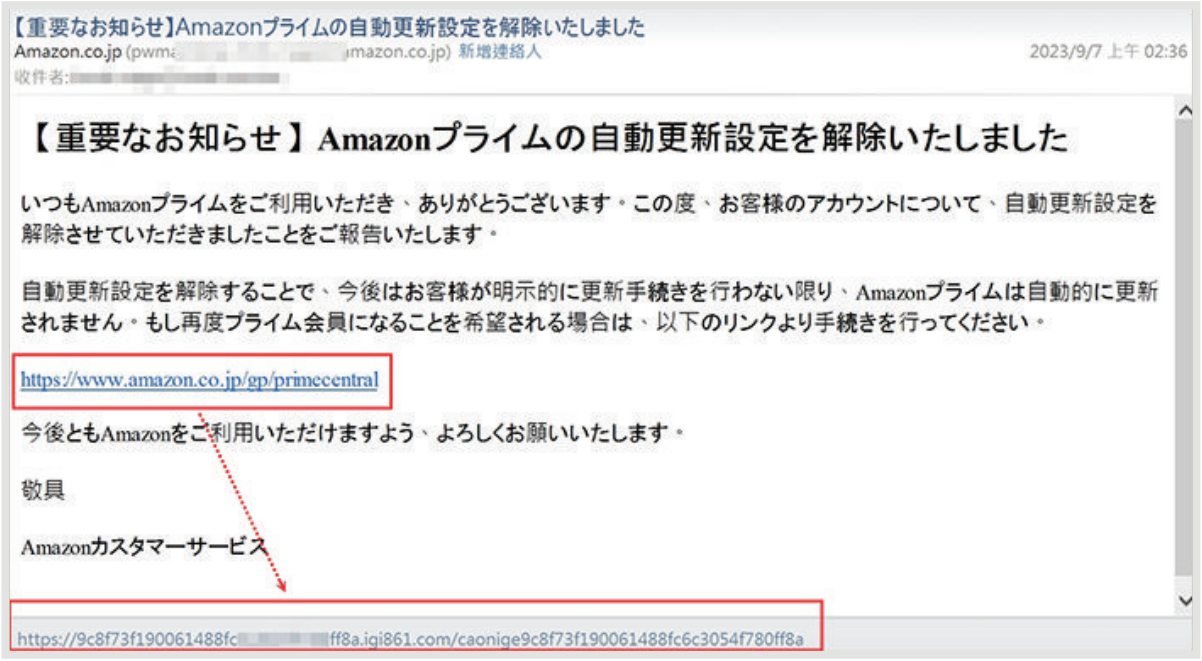
Spam Mail
Virus Mail
Malicious Mail

Oct 2023 released.

在第三季，我們發現郵件內帶有惡意連結的情況較上一季增加了 60%；垃圾郵件的大小與 419scam 的數量，與上一季相較都減少了 30% 左右，釣魚郵件是本季最主要的攻擊。以下是本季幾個特殊的樣本：
本季特殊郵件攻擊樣本解析：

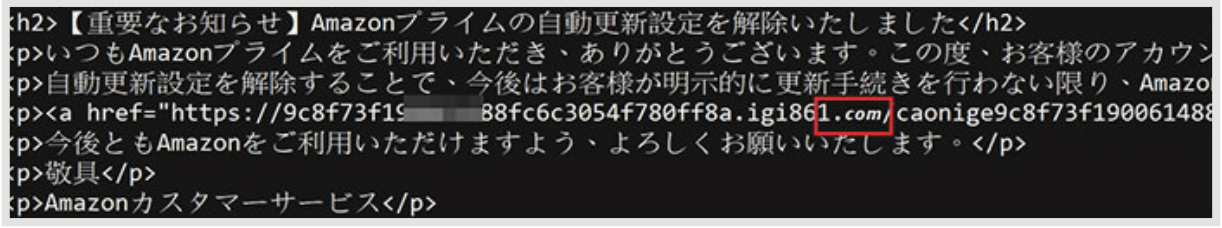
透過字元變換躲避偵測的釣魚郵件

在第三季，我們觀察到一個特別的釣魚郵件。這個釣魚郵件冒充了 Amazon 通知信，並且出現了一般釣魚郵件常見的特徵：顯示的連結與真實前往的連結不一致。



一般釣魚郵件常見的特徵：顯示的連結與真實前往的連結不一致

特別的是，若是直接檢視這封釣魚郵件的原始檔，會發現有些字元顯示的樣子有種違和感。



檢視這封釣魚郵件的原始檔，會發現 .com 的顯示似乎與其他英文字元不太一致

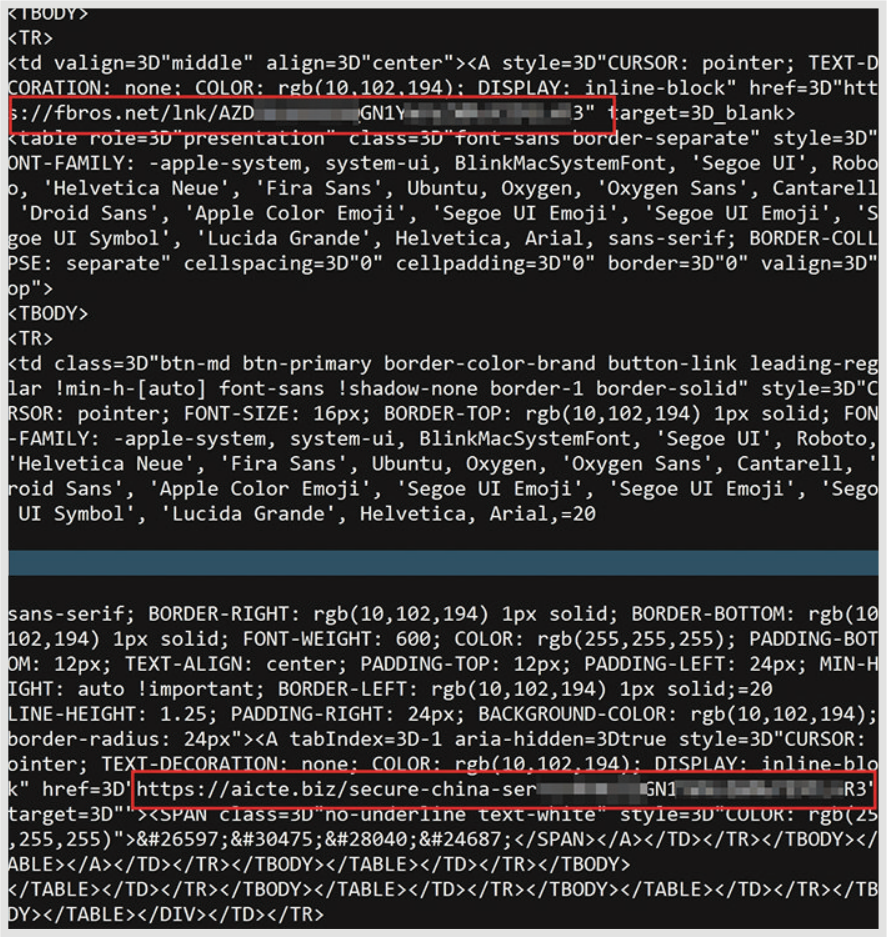
這是因為攻擊使用 Unicode 字元替換域名中的部分字元。攻擊者也能對郵件內惡意連結中的域名做其他改變，例如：將小寫字母切換為大寫字母，或塞入不可見字元...等，藉此繞過資料庫的比對判斷，而這樣的手法對於瀏覽器、收信軟體，都還是能夠解析為可被收件者點擊的惡意域名網址。

一個按鈕兩個釣魚連結

我們也發現了一個奇怪的案例：一封偽冒 Linkedin 的釣魚郵件，在同一個按鈕中，潛藏了兩個釣魚連結。透過在按鈕上操作滑鼠移動，可以看見兩個超連結的切換。

這兩個超連結連往的是不同的伺服器，似乎都是被入侵的網站，而在其網站支系的某個目錄，藏有轉址程式碼，會將上鉤的受害人連往另一個被入侵的釣魚網址，例如：hxxps://cendas.com.ar/wp-content/china/chinaserver-LINKEDIN/# (受害者以 base64 編碼的 E-mail Address)，同時在一個按鈕設置兩個釣魚連結，可能是為了逃過封鎖，提高釣魚的成功機率。

常見的偽冒釣魚郵件



```
<TBODY>
<TR>
<td valign=3D"middle" align=3D"center"><A style=3D"CURSOR: pointer; TEXT-D
CORATION: none; COLOR: rgb(10,102,194); DISPLAY: inline-block" href=3D"htt
s://fbros.net/lnk/AZD                GN1Y                3" target=3D_blank>
<table role=3D"presentation" class=3D"font-sans border-separate" style=3D"
ONT-FAMILY: -apple-system, system-ui, BlinkMacSystemFont, 'Segoe UI', Robo
o, 'Helvetica Neue', 'Fira Sans', Ubuntu, Oxygen, 'Oxygen Sans', Cantarell
 'Droid Sans', 'Apple Color Emoji', 'Segoe UI Emoji', 'Segoe UI Emoji', 'S
goe UI Symbol', 'Lucida Grande', Helvetica, Arial, sans-serif; BORDER-COLL
PSE: separate" cellspacing=3D"0" cellpadding=3D"0" border=3D"0" valign=3D"
op">
<TBODY>
<TR>
<td class=3D"btn-md btn-primary border-color-brand button-link leading-reg
lar !min-h-[auto] font-sans !shadow-none border-1 border-solid" style=3D"C
RSOR: pointer; FONT-SIZE: 16px; BORDER-TOP: rgb(10,102,194) 1px solid; FON
-FAMILY: -apple-system, system-ui, BlinkMacSystemFont, 'Segoe UI', Roboto,
'Helvetica Neue', 'Fira Sans', Ubuntu, Oxygen, 'Oxygen Sans', Cantarell, '
roid Sans', 'Apple Color Emoji', 'Segoe UI Emoji', 'Segoe UI Emoji', 'Sego
 UI Symbol', 'Lucida Grande', Helvetica, Arial,=20

sans-serif; BORDER-RIGHT: rgb(10,102,194) 1px solid; BORDER-BOTTOM: rgb(10
102,194) 1px solid; FONT-WEIGHT: 600; COLOR: rgb(255,255,255); PADDING-BOT
OM: 12px; TEXT-ALIGN: center; PADDING-TOP: 12px; PADDING-LEFT: 24px; MIN-H
IGHT: auto !important; BORDER-LEFT: rgb(10,102,194) 1px solid;=20
LINE-HEIGHT: 1.25; PADDING-RIGHT: 24px; BACKGROUND-COLOR: rgb(10,102,194);
border-radius: 24px"><A tabIndex=3D-1 aria-hidden=3Dtrue style=3D"CURSOR:
pointer; TEXT-DECORATION: none; COLOR: rgb(10,102,194); DISPLAY: inline-blo
k" href=3D'https://aicte.biz/secure-china-ser          GN1          R3'
target=3D"_"><SPAN class=3D"no-underline text-white" style=3D"COLOR: rgb(25
,255,255)">&#26597;&#30475;&#28040;&#24687;</SPAN></A></TD></TR></TBODY></
ABLE></A></TD></TR></TBODY></TABLE></TD></TR></TBODY>
</TABLE></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR></TB
DY></TABLE></DIV></TD></TR>
```

檢視原始檔後，可看見連往兩個不同的釣魚網站

複合釣魚手段

接下來這封偽冒電商的詐騙郵件複合了多重技巧。先以社交工程的手段聲稱該電商無法驗證用戶的信用卡，可能造成用戶消費的困擾，接著明確顯示電商的超連結，但實際連線到遭入侵的釣魚網頁，這是釣魚郵件常見手段。

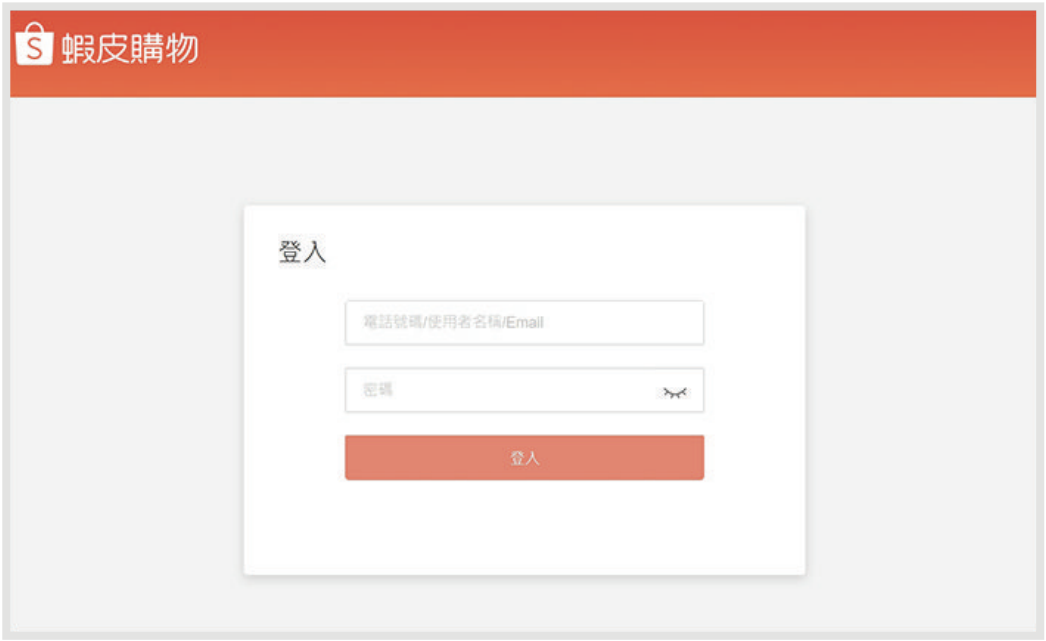
偽冒電商的詐騙郵件

檢視原始檔，我們發現攻擊者在郵件中藏入一張長寬為 1 的圖片，圖片來源為 [[TRACKINGPIXEL]]，可能是攻擊者忘了將釣魚樣板定義的變數替換成追蹤連結。但若此處被置入一個有效的追蹤連結，當用戶開啟這封郵件時，若沒有封鎖圖片，則會通知統計的主機記錄這封信的所有開信者訊息，包括時間、IP、MUA 版本，並且讓攻擊者知道攻擊對象的防護狀態...等相關資料。

```
</td>
</tr>
</tbody>
</table>
<div><img style=3D"position: absolute; visibility: hidden;" src=3D"about:bl=
ank" width=3D"0" height=3D"0" border=3D"0" /></div>
<img src=3D"%5B%5BTRACKINGPIXEL%5D%5D" width=3D"1" height=3D"1" border=3D"0=
" /></td>
</tr>
</tbody>
```

攻擊者忘了將釣魚樣板定義的變數替換成追蹤連結

當受害者不察，連往釣魚網頁時，第一步將被騙取的是使用於電商的帳號密碼。在這個階段，不論輸入的帳號密碼為何，都會被攻擊者紀錄後，成功跳轉至下一個頁面；遭到盜取的帳號密碼則可能用於後續其他的攻擊。



第一步將被騙取的是使用於電商的帳號密碼

第二步是騙取信用卡的相關資料。在這個階段，受害者為了購物便利，可能會受騙新增信用卡。巧妙的是，在此頁面不論輸入任何信用卡資料，在送出後都會被攻擊者紀錄，接著顯示「出現錯誤　請輸入卡號」的提示，並且清空信用卡資料的相關欄位，受害者可能在情急之下，換另一張卡輸入，有可能因此被連續竊取多張信用卡資料。這個遭到入侵的釣魚網站，直至截稿前仍在運行。

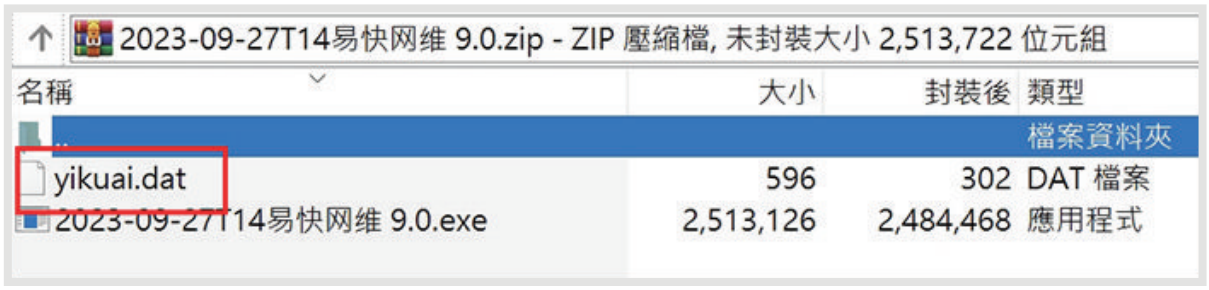
受害者可能在情急之下換另一張卡輸入，因此連續被竊取多張信用卡的資料

留意遠端遙控、維護軟體的濫用情況

這一季也發現有攻擊者試圖以社交工程的方式，操控受害者安裝遠端遙控、維護軟體用於不明用途。首先，在郵件中完全未提及遠端遙控、維護軟體的資訊，巧妙的將遙控軟體放置於外部連結，躲避郵件掃描的檢測。

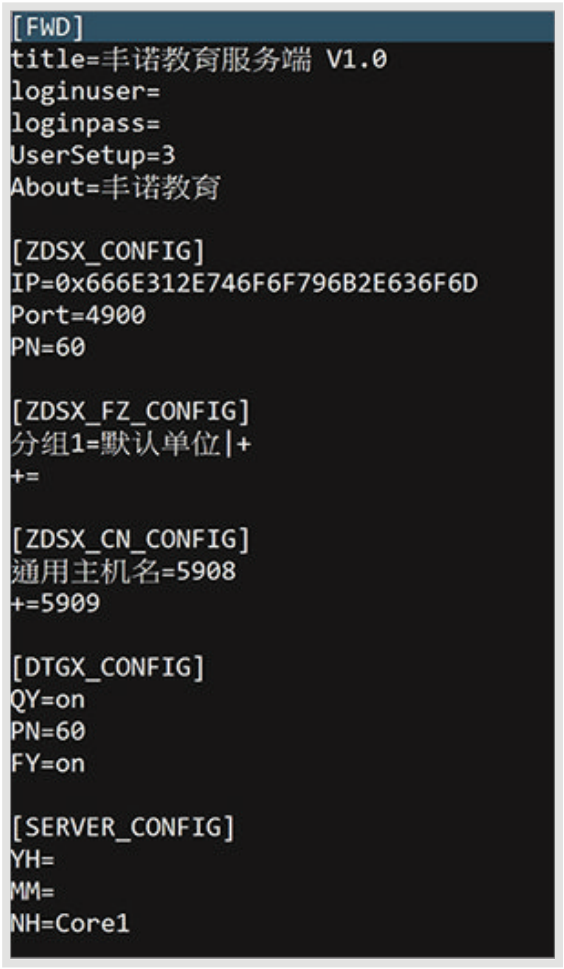
將遙控軟體放置於外部連結，躲避郵件掃描的檢測

當受害者下載了遙控軟體壓縮檔後，攻擊者將遙控軟體的設定檔設定為隱藏檔；因此在 Windows 的預設情況下，解壓縮出來的檔案看起來只有一個遙控軟體。



遙控軟體的設定檔被攻擊者設定為隱藏檔

查看設定檔的內容就能發現這個設定檔並不單純，除了改變安裝軟體顯示的標題外，也將連接的 IP、通訊埠都設定好了，在安裝完成後，也能在受害者無法察覺的情況下，遠端監控、操作受害者的電腦。而這個遙控軟體本來的遠端維修用途，未必會被所有的防毒軟體視為有害。



```
[FWD]
title=丰诺教育服务端 V1.0
loginuser=
loginpass=
UserSetup=3
About=丰诺教育

[ZDSX_CONFIG]
IP=0x666E312E746F6F796B2E636F6D
Port=4900
PN=60

[ZDSX_FZ_CONFIG]
分组1=默认单位|+
+=

[ZDSX_CN_CONFIG]
通用主机名=5908
+=5909

[DTGX_CONFIG]
QY=on
PN=60
FY=on

[SERVER_CONFIG]
YH=
MM=
NH=Core1
```

查看設定檔的內容就會發現這個設定檔並不單純

結論

在這一季，雖然有漏洞被揭露，但似乎尚未遭到大規模的利用，整體仍以釣魚郵件為主要攻擊主軸。釣魚郵件顧名思義，目標就是要釣取後續可以再利用的資訊；釣魚郵件除了不停的進化出各種能規避偵測的技術，近期，我們也注意到釣魚郵件的攻擊者更加專注於遭到釣魚的目標，諸如：開信、是否上鉤、釣取資料的有效性、更多可以一併得到的目標資訊。這些遭到釣取的機敏資訊都可以再組合、拼湊並且重複被使用，或結合詐騙、偽造身分等攻擊。做好資安，切莫輕忽釣魚郵件！

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