


**TLP:WHITE**



# 竊取信用卡卡號之釣魚信件 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2021 年 05 月

## 一、事件簡介

2021/3 初至 2021/4 中旬 TACERT 的 Service 信箱陸續接到 6 封偽裝來自中華郵政的釣魚信件，這些信件以包裹無法送達是因為沒有繳納關稅(369 元台幣)的名義寄出。為了瞭解這些釣魚信的詐騙行為，本中心對這 6 封信件進行檢測。

名稱	修改日期
✉ 您的包裹無法在2021年03月02日送達 Fwd Your package could not be delivered on 02.03.2021.msg	2021/3/11 上午 11:10
✉ 您的包裹無法在2021年03月02日送達 Fwd Your package could not be delivered on 02.03.2021 ID51009RANDRAND.msg	2021/3/11 上午 11:11
✉ Fwd : 您的包裹無法送達 30.03.2021 □.msg	2021/3/30 下午 12:48
✉ 中華郵政-您的包裹無法送達.msg	2021/4/9 上午 10:11
✉ Fwd : 您的包裹無法送達.msg	2021/4/9 上午 10:20
✉ 您的包裹無法送達 04192021 023954 am.msg	2021/4/19 上午 10:26

## 二、事件檢測

1. 首先，依照信件收信時間對信件依序編號第 1~6 號如下。

信件編號	收信日期	寄件者信箱
1	2021/3/2 下午 01:56	Chunghwa Post   中華郵政 ✓ <support9104186180429756842@mm.syria.press>
2	2021/3/2 下午 04:53	Chunghwa Post   中華郵政 ✓ <support0a2e2fa045bf15ab1372272cbde69d95@andrea-weigel.de>
3	2021/3/26 下午 05:39	中華郵政 <iniu54905652@web-worker-linux.whservidor.com>
4	2021/3/30 上午 10:00	Chunghwa Post   中華郵政 <support4c2x8j2v967pqmg01@hustlersedition.com>
5	2021/4/8 上午 08:46	中華郵政 <dev54395186@mundialcc.com.br>
6	2021/4/19 上午 08:40	中華郵政 ✓ <support@elmhandball.de>

本次檢測將以第 6 封信件為主要檢測對象，並且與其他 5 封信件進行特徵比對，以了解駭客在製作釣魚信件的手法。

2. 開啟第 6 封信件得知：

- (1) 該信件以「中華郵政客戶服務」名義自 support@elmhandball.de 寄出信件。
- (2) 該信告訴收信者您的包裹因為沒有繳納關稅 369 元故無法交付。

(3) 提供商家名稱與訂單號碼企圖取信收件者。

(4) 提供確認包裹運輸情況與後續處理情形的連結給收信者查詢。

2021/4/19 (週一) 上午 08:40  
中華郵政 <support@elmhandball.de>  
您的包裹無法送達 04/19/2021 02:39:54 am  
收件者 service@cert.tanet.edu.tw  
如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

你好，

最後提醒：該電子郵件通知您的貨件仍在等待處理中。

您的包裹無法在交付 **19.04.2021** 因為沒有繳納關稅 ( 369 NT Dollars)

商家：中華郵政  
訂單號碼：00275029  
採購金額：369 新台幣  
計劃於 21.04.2021-22.04.2021 之間交付

- 確認包裹的運輸 [點擊這裡](#)。

當您到達家庭住址時，您將收到一封電子郵件或短信。從可用之日起，您將有 8 天的時間撤消包裹。提款後，系統會要求您提供 ID。

- 如需更多服務，請通過以下方式查找您的貨件的後續行動 [點擊這裡](#)。

謝謝您的信任，

真摯地，  
您的中華郵政客戶服務。

3. 第 6 封信件內兩個「點擊這裡」的連結網址皆相同，點擊後會先開啟

「<http://quantum-dental.de/wp.php>」。之後會轉址至信用卡付款頁面

(<https://fmbpda.com/kio/Twa/internet/Group/f42cb/SSLAuthUI.html>)，來提供收

信者以信用卡支付 369 元的付款管道。

商家：中華郵政  
訂單號碼：00275029  
採購金額：369 新台幣  
計劃於 21.04.2021-22.04.2021 之間交付 <http://quantum-dental.de/wp.php>  
按一下以追蹤連結

- 確認包裹的運輸 [點擊這裡](#)。

當您到達家庭住址時，您將收到一封電子郵件或短信。從可用之日起，您將有 8 天的時間撤消包裹。提款後，系統會要求您提供 ID。

商家：中華郵政  
訂單號碼：00275029  
採購金額：369 新台幣  
計劃於 21.04.2021-22.04.2021 之間交付

- 確認包裹的運輸 [點擊這裡](#)。

當您到達家庭住址時，您將收到一封電子郵件或短信。從可用之日起，<http://quantum-dental.de/wp.php> 後，系統會要求您提供 ID。  
按一下以追蹤連結

- 如需更多服務，請通過以下方式查找您的貨件的後續行動 [點擊這裡](#)。

謝謝您的信任，

**轉址**  
<https://fmbpda.com/kio/Twa/internet/Group/f42cb/SSLAuthUI.html>

信用卡付款頁面

fmbpda.com/kio/Twa/internet/Group/48752/SSLAuthUI.html

**中國信託銀行**  
CTBC BANK

VISA MasterCard JCB  
我們接受VISA、MasterCard、JCB之信用卡交易！

歡迎您光臨本行特約商店：**Postal Stamps Mall**  
您採用本行 SSL PLUS 網路交易安全機制付款！

訂單編號  
Order Number 00275029

訂單金額  
Purchase Amount 369 新台幣  
NT Dollars

信用卡號  
Credit Card Number XXXX XXXX XXXX XXXX

三碼檢查碼  
3-digital Card Validation Code ... 背面後三碼檢查碼 ⓘ

信用卡到期[月/年]  
Expire Date [Month/Year] MM / YYYY

確認付款 To Pay

4. 填入信用卡資訊後，按確認付款送出。接著會出現使用手機簡訊進行密碼驗證的視窗訊息。

訂單編號  
Order Number 00275029

訂單金額  
Purchase Amount 369 新台幣  
NT Dollars

信用卡號  
Credit Card Number 1234567891234567

三碼檢查碼  
3-digital Card Validation Code 678 背面後三碼檢查碼 ⓘ

信用卡到期[月/年]  
Expire Date [Month/Year] 11 / 2026

確認付款 To Pay

**中華郵政全球資訊網**  
Chunghwa Post Co., Ltd.

Order Number 訂單編號 : 00275029  
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars  
21.04.2021

Please do not close this window before completing this step. The process may take a few seconds. Thank you for your patience

完成此步驟之前，請不要關閉此窗口。該過程可能需要幾秒鐘。感謝您的耐心等待



5. 在手機簡訊進行密碼驗證方面，若驗證失敗會出現驗證失敗訊息。該訊息警告收信者若輸入3次錯誤代碼，除當前交易被取消外，信用卡也會被凍結。經檢測發現，輸入3次(含)以上錯誤代碼後，並無任何異常現象，推測此為詐騙收信者要輸入正確的信用卡資訊的手法。

中華郵政全球資訊網  
Chunghwa Post Co., Ltd.

Order Number 訂單編號 : 00275029  
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars  
21.04.2021

Please confirm the following payment  
請確認以下付款

The unique password has been sent to the mobile number below. If you need to change your mobile number, please contact your bank or change it through the available channels (ATM, web).

唯一密碼已發送到下面的手機號碼。如果您需要更改手機號碼，請與您的銀行聯繫或通過可用的渠道（ATM，網絡）進行更改。

確認付款 To Pay

中華郵政全球資訊網  
Chunghwa Post Co., Ltd.

Order Number 訂單編號 : 00275029  
Purchase Amount 訂單金額 : 369 新台幣 NT Dollars  
21.04.2021

Please confirm the following payment  
請確認以下付款

The unique password has been sent to the mobile number below. If you need to change your mobile number, please contact your bank or change it through the available channels (ATM, web).

唯一密碼已發送到下面的手機號碼。如果您需要更改手機號碼，請與您的銀行聯繫或通過可用的渠道（ATM，網絡）進行更改。

SMS is wrong or expired! After (3) errors when entering the code received via SMS, the current transaction is canceled and the credit card is blocked.

短信錯誤或已過期！輸入通過SMS接收到的代碼後出現（3）錯誤後，當前交易被取消，信用卡被凍結。

確認付款 To Pay

6. 第6封信之信件連結網址(<http://quantum-dental.de/wp.php>)在2021/4/21經VirusTotal檢測其惡意比例為0/87，但在2021/5/3再次檢測時其惡意比例變為2/87。有兩家防毒軟體公司的防毒軟體判定該網址為釣魚網址或是惡意網址。


2 / 87

2 security vendors flagged this URL as malicious

<http://quantum-dental.de/wp.php> 404 text/html; charset=iso-8859-1 2021-05-03 06:13:37 UTC  
quantum-dental.de Status Content Type a moment ago

Fortinet Phishing SCUMWARE.org Malware


轉址網址(<https://fmbpda.com/kio/Twa/internet/Group/f42cb/SSLAuthUI.html>)經VirusTotal檢測其惡意比例為11/87。

		11 security vendors flagged this URL as malicious	
<a href="https://fmbpda.com/kio/Twa/Internet/Group/f42cb/SSLAAuthUI.html">https://fmbpda.com/kio/Twa/Internet/Group/f42cb/SSLAAuthUI.html</a>		200	text/html
fmbpda.com		Status	Content Type
		2021-04-21 16:32:47 UTC	
		14 days ago	

AegisLab WebGuard	Phishing	Avira (no cloud)	Phishing
BitDefender	Malware	CRDF	Malicious
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	Fortinet	Phishing
Netcraft	Malicious	SCUMWARE.org	Malware
Sophos	Phishing	ADMINUSLabs	Clean

7. 在第 6 封信之信件內容最後面若往下看，經過一段空白後會出現以 DHL 公司名義所寫的信件內容，推測這內容可能為詐騙信件草稿。此段隱藏訊息告訴收件者在 14 天內需支付 199 歐元來取得包裹，一樣提供點選的連結 (<https://administrativos.cl/wp.php>)給使用者點選。點連結後發現已無法開啟該網頁。


2021/4/19 (週一) 上午 08:40  
中華郵政 <support@elmhandball.de>  
您的包裹無法送達 04/19/2021 02:39:54 am

收件者 service@cert.tanet.edu.tw

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

**Dear Customer,**

Your package is waiting for delivery, Please confirm the payment **(1,99EUR)** on the link below the online verification needs to be done in the next 14 days before it expires:

<https://administrativos.cl/wp.php>  
按一下以追蹤連結

**Follow my package**

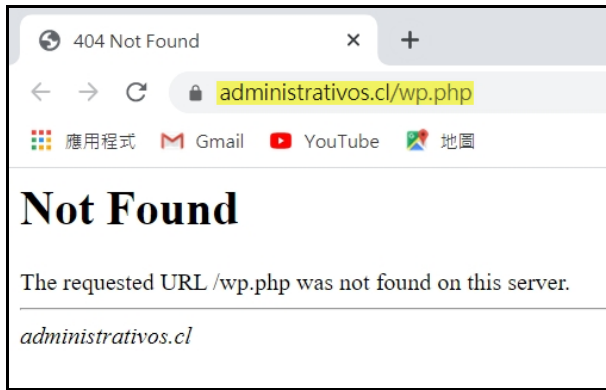
This email is provided for informational purposes only and does not guarantee delivery of the shipment. Unable to reply to this email. Your e-mail address will only be used for the announcement of the parcel of the above shipment and will not be saved for advertising purposes. If you no longer wish to receive the package announcement, please click here: [DHL Notification Service](#)

---

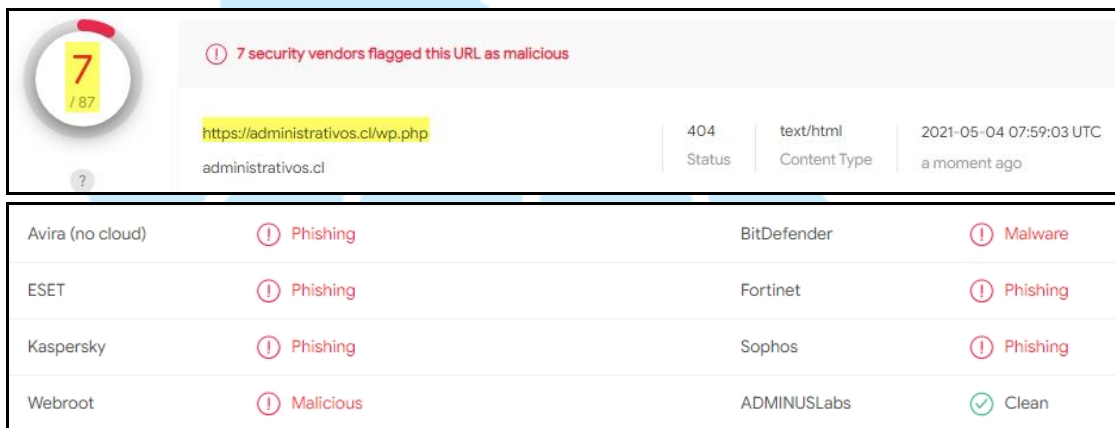
[Website](#) [Contact](#) [Impressum](#)

© 2020 DHL

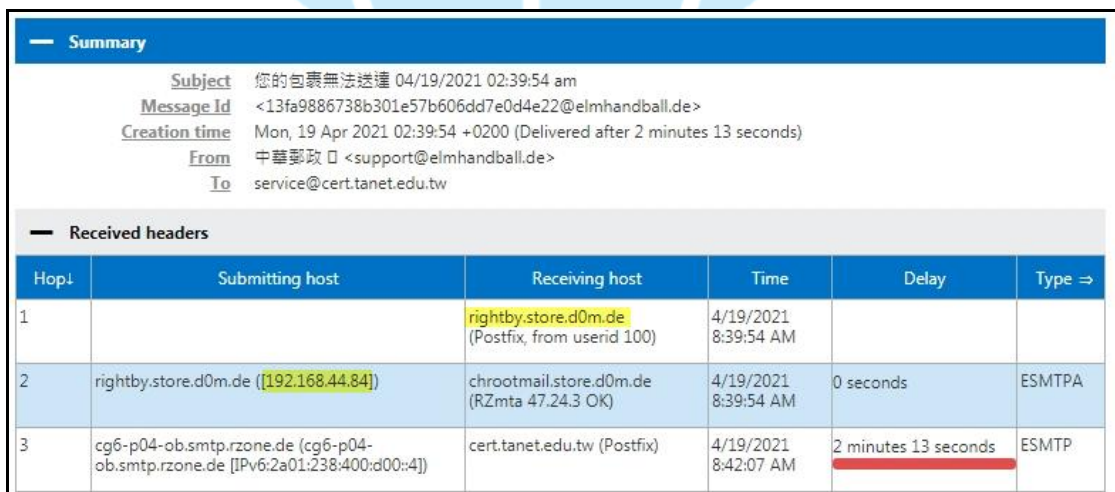




該網址(https://administrativos.cl/wp.php)經 Virustotal 檢測後發現其惡意比例為 7/87。



8. 檢視第 6 封信之 Mail Header 內容，發現信件一開始是從 rightby.store.d0m.de(IP:192.168.44.84)的郵件伺服器寄出。經過一次轉信後由 cg6-p04-ob.smtp.rzone.de 寄至 TACERT 的郵件伺服器，由這些郵件伺服器資訊可以得知信件來自德國。



Other headers		
#	Header	Value
1	Return-Path	<support@elmhandball.de>
2	X-Original-To	service@cert.tanet.edu.tw
3	Delivered-To	service@cert.tanet.edu.tw
4	DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; t=1618792795; s=strato-dkim-0002; d=elmhandball.de; h=Message-ID:From:Date:Subject:To:Cc:Date:From:Subject:Sender; bh=N3r8+8ksSqHixTAyFj1AOocyZ96gmwL8jt3PCgRUzqw=; b=A9IGtoOh52k+ebC+d+56osy4VfmN0PBKJksXMxMGngTxq6u/qNedx5L8Hij8as2BN ZHHzk4QWDWTAPEpRkpt3Qo6tXyn/iGftx0Fluo5dq+uBwFgFcGoAbDxueyZ3X8cmQk33 hks1Qr7WW0dDgpyxbP8b8/gqDvZZd7oAPELnXJCHa/b78Xbcv67esztHs5HMCxFCbSxq rQ1Z/5uKQvE4Wrc7AJ6DVUYU+8F8I2LnXvqt5b8BDNYLVDINX30o3RduCOLhaX4r1SKYcBggOccnQiV+QracZWcMh18gVkhLAymxuqWOn2Q5Spfmdqb/kK/zfCcZm1Q9/tv454 TCWA==

9. 檢測第 1~5 封信件內容如下。

- (1) 第 1 封信：該信件在 2021/3/2 下午 01:56 被寄出，而且信件內容與第 6 封信件內容相同，僅差別在第 1 封信內容為英文版。第 1 封信的信件連結網址(<http://pre.asocs.info/wp-maill.php>)經 Virustotal 檢測其惡意比例為 0，但是點選該連結後會轉址至「<https://www.afraso.org/sites/all/new.php?id=64406665>」的網站。



2021/3/2 (週二) 下午 01:56  
**Chunghwa Post | 中華郵政** <support9104186180429756842@mm.syria.press>  
 您的包裹無法在2021年03月02日送達 | Fwd: Your package could not be delivered on 02.03.2021 ID51009[RAND][RAND]

收件者 service@cert.tanet.edu.tw  
 ⓘ 如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

✕

**Hello ,**

**Last Reminder:** This Email informs you that your shipment is still pending.

Your package could not be delivered on **02.03.2021** because no customs duty was paid ( **369 NT Dollars**)

**Merchant : Chunghwa Post**  
**Order Number : 00275029**  
**Purchase Amount : 369 NT Dollars**  
**Delivery scheduled between : 03.03.2021 - 04.03.2021** <http://pre.asocs.info/wp-maill.php>  
 按一下以追蹤連結

- To confirm the shipment of your package [Click here](#).

You will \_\_\_\_receive \_\_\_\_an \_\_\_\_email \_\_\_\_or \_\_\_\_SMS \_\_\_\_when \_\_\_\_you \_\_\_\_arrive in your \_\_\_\_home \_\_\_\_address. You will \_\_\_\_have 8 days, from \_\_\_\_the date \_\_\_\_of \_\_\_\_availability, to \_\_\_\_withdraw the package. \_\_\_\_Upon withdrawal, \_\_\_\_you will be \_\_\_\_asked for ID.

- For more services, find the follow-up of your shipment by [Clicking here](#).

Thank you for your trust,

Sincerely,  
 Your **Chunghwa Post** customer service.

Compensation  
 Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy, being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy. The Company hereby declaring the following statements in regards with the collection, processing.

轉址的網址「<https://www.afraso.org/sites/all/new.php?id=64406665>」經

Virustotal 檢測其惡意比例為 2/87，僅兩家防毒軟體公司的防毒軟體可檢測出其為釣魚網站。



2 security vendors flagged this URL as malicious

<https://www.afraso.org/sites/all/new.php?id=64406665>

404 Status

text/html; charset=utf-8 Content Type

2021-05-03 06:51:55 UTC a moment ago

Comodo Valkyrie Verdict

Phishing

Fortinet

Phishing

檢視第 1 封信的 MailHeader 發現該信件寄件者 IP 為來自德國

IP:46.4.227.78。

Summary

Subject

Message Id

Creation time

From

To

您的包裹無法在2021年03月02日送達 | Fwd: Your package could not be delivered on 02.03.2021 ID51009[RAND][RAND]

<77cff437b1666f917ba3f34ce78e169c@mm.syria.press>

Tue, 2 Mar 2021 05:55:39 +0000 (Delivered after -4 minutes 14 seconds)

Chunghwa Post | 中華郵政 <support9104186180429756842@mm.syria.press>

service@cert.tanet.edu.tw

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type
1	al3al	host.yalagroup.net	3/2/2021 1:55:39 PM		local (Exim 4.93) (envelope-from <support9104186180429756842@mm.syria.press>)
2	static.78.227.4.46.clients.your-server.de (static.78.227.4.46.clients.your-server.de [46.4.227.78])	cert.tanet.edu.tw (Postfix)	3/2/2021 1:51:25 PM	-4 minutes 14 seconds	ESMTP

(2) 第 2 封信:信件內容與信件連結網址皆與第 1 封信相同。

2021/3/2 (週二) 下午 04:53

Chunghwa Post | 中華郵政 <support0a2e2fa045bf15ab1372272cbde69d95@andrea-weigel.de>

您的包裹無法在2021年03月02日送達 | Fwd: Your package could not be delivered on 02.03.2021

收件者 service@cert.tanet.edu.tw

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

Hello ,

**Last Reminder:** This Email informs you that your shipment is still pending.

Your package could not be delivered on **02.03.2021** because no customs duty was paid ( **369 NT Dollars** )

**Merchant : Chunghwa Post**  
**Order Number : 00275029**  
**Purchase Amount : 369 NT Dollars**  
**Delivery scheduled between : 03.03.2021 - 04.03.2021**

<http://pre.asocs.info/wp-mail.php>  
 按一下以追蹤連結

- To confirm the shipment of your package [Click here](#).

You will receive an email or SMS when you arrive in your home address. You will have 8 days, from the date of availability, to withdraw the package. Upon withdrawal, you will be asked for ID.

- For more services, find the follow-up of your shipment by [Clicking here](#).

Thank you for your trust,

Sincerely,  
 Your **Chunghwa Post** customer service.

Compensation  
 Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy, being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy. The Company hereby declaring the following statements in regards with the collection, processing,

檢視第 2 封信的 MailHeader 發現該信件寄件者 IP 為來自德國 IP:

81.169.211.109。

Summary

Subject

Message Id

Creation time

From

To

您的包裹無法在2021年03月02日送達 | Fwd: Your package could not be delivered on 02.03.2021

<681c7b27db847c2d19c1c43e35fe770d@andrea-weigel.de>

Tue, 2 Mar 2021 08:53:05 +0000 (Delivered after -4 minutes 1 second)

Chunghwa Post | 中華郵政 <support0a2e2fa045bf15ab1372272cbde69d95@andrea-weigel.de>

service@cert.tanet.edu.tw

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type⇒
1		h2644144.stratoserver.net (Postfix, from userid 10028)	3/2/2021 4:53:05 PM		
2	andrea-weigel.de (nrwdo.de [81.169.211.109])	cert.tanet.edu.tw (Postfix)	3/2/2021 4:49:04 PM	-4 minutes 1 second	ESMTP

- (3) 第 3 封信:該信件在 2021/3/26 下午 05:39 被寄出,其信件內容與第 1 封信、第 2 封信相同,僅中、英文版的差異。信件連結網址 (<https://cursedanarchy.com/new.php>)經 Virustotal 檢測其惡意比例為 1/87, 有一家防毒軟體公司認為其為惡意網址。

1 / 87				
1 security vendor flagged this URL as malicious				
<a href="https://cursedanarchy.com/new.php">https://cursedanarchy.com/new.php</a>	404	text/html	2021-05-03 03:09:34 UTC	
cursedanarchy.com	Status	Content Type	a moment ago	

SCUMWARE.org	Malware	Fortinet	Spam
--------------	---------	----------	------

2021/3/26 (週五) 下午 05:39  
**中華郵政** <iniu54905652@web-worker-linux.whservidor.com>  
**Fwd: 您的包裹無法送達**

收件寄 service@cert.tanet.edu.tw  
如果這個訊息的顯示有任何問題,請按一下這裡,在網頁瀏覽器中檢視。

訊息 未命名的附件 00676.txt

你好,

**最後提醒:** 該電子郵件通知您的貨件仍在等待處理中。

您的包裹無法在交付 **26.03.2021** 因為沒有繳納關稅 ( 369 NT Dollars)

**商家: 中華郵政**  
**訂單號碼: 00275029**  
**採購金額: 369 新台幣**  
**計劃於 27.03.2021-28.03.2021** <https://cursedanarchy.com/new.php>  
按一下以追蹤連結

- 確認包裹的運輸 [點擊這裡](#).

當您到達家庭住址時,您將收到一封電子郵件或短信。從可用之日起,您將有 8 天的時間撤消包裹。提款後,系統會要求您提供 ID。

- 如需更多服務,請通過以下方式查找您的貨件的後續行動 [點擊這裡](#).

謝謝您的信任,

真摯地,  
您的中華郵政客戶服務。

Compensation  
Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy, being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy. The Company hereby declaring the following statements in regards with the collection, processing,

檢視第 3 封信的 MailHeader 發現該信件寄件者 IP 為來自兩個德國 IP:

195.225.209.16、195.158.54.3。

Summary

Subject

Fwd: 您的包裹無法送達

Message Id

<20210326093839.202AD2D5752@c3.confixx.webjanssen.de>

Creation time

Fri, 26 Mar 2021 10:38:39 +0100 (CET) (Delivered after 0 seconds)

From

中華郵政 <iniu54905652@web-worker-linux.whservidor.com>

To

service@cert.tanet.edu.tw

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type →
1		c3.confixx.webjanssen.de (Postfix, from user id 664)	3/26/2021 5:38:39 PM		
2	[195.225.209.16]	wjoutfilter	3/26/2021 5:38:26 PM	-13 seconds	Xeams SMTP
3	wjoutfilter.webjanssen.de (wjoutfilter.webjanssen.de [195.158.54.3])	cert.tanet.edu.tw (Postfix)	3/26/2021 5:38:39 PM	13 seconds	ESMTP

- (4) 第 4 封信: 該信件在 2021/3/30 上午 10:00 被寄出，其信件內容與第 3 封信相同。信件連結網址(<http://pixlfeed.com/wp-admin/user/wp.php>)經 Virustotal 檢測其惡意比例為 0/87。

2021/3/30 (週二) 上午 10:00

**Chunghwa Post | 中華郵政** <support4c2x8j2v967pqmg01@hustlersedition.com>

**Fwd: 您的包裹無法送達 30.03.2021**

收件者: service@cert.tanet.edu.tw

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

訊息 AT00001.txt

你好，

**最後提醒：** 該電子郵件通知您您的貨件仍在等待處理中。

您的包裹無法在交付 30.03.2021 因為沒有繳納關稅 ( 369 NT Dollars)

商家：中華郵政  
 訂單號碼：00275029  
 採購金額：369 新台幣  
 計劃於 31.03.2021-01.04.2021

<http://pixlfeed.com/wp-admin/user/wp.php>  
 按一下以追蹤連結

- 確認包裹的運輸 [點擊這裡](#)。

當您到達家庭住址時，您將收到一封電子郵件或短信。從可用之日起，您將有 8 天的時間撤消包裹。提款後，系統會要求您提供 ID。

- 如需更多服務，請通過以下方式查找您的貨件的後續行動 [點擊這裡](#)。

謝謝您的信任，

真摯地，  
 您的中華郵政客戶服務。

Compensation  
 Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy, being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy. The Company hereby declaring the following statements in regards with the collection, processing,

0 / 87

No security vendors flagged this URL as malicious

<a href="http://pixlfeed.com/wp-admin/user/wp.php">http://pixlfeed.com/wp-admin/user/wp.php</a>	504	text/html	2021-05-03 06:00:58 UTC
pixlfeed.com	Status	Content Type	1 minute ago

檢視第 4 封信的 MailHeader 發現該信件寄件者 IP 為來自美國 IP:  
74.208.58.198 與德國 IP: 82.165.159.134。

Summary

Subject

Fwd : 您的包裹無法送達 30.03.2021 □

Message Id

<292aea38811258716babf0f2f36ee79f@hustlersedition.com>

Creation time

Mon, 29 Mar 2021 21:59:52 -0400 (Delivered after 3 seconds)

From

Chunghwa Post | 中華郵政 <support4c2x8j2v967pqmg01@hustlersedition.com>


To

service@cert.tanet.edu.tw

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type →
1	localhost [74.208.58.198]	mrelay.perfora.net (mreueus003 [74.208.5.2])	3/30/2021 9:59:53 AM		ESMTPSA (Nemesis)
2	mout-xforward.perfora.net (mout-xforward.perfora.net [82.165.159.134])	cert.tanet.edu.tw (Postfix)	3/30/2021 9:59:56 AM	3 seconds	ESMTP

- (5) 第 5 封信:該信件在 2021/4/8 上午 08:46 被寄出，而且信件內容與第 3 封信、第 4 封信相同。信件連結網址(<https://www.jonkeinteriors.co.za/web.php>)經 Virustotal 檢測其惡意比例為 3/87，但是點選該連結後會轉址至「<https://www.matchandshare.nl/home/Twa/internet/Group/?id=87854917>」的網站。



2021/4/8 (週四) 上午 08:46

中華郵政 <dev54395186@mundialcc.com.br>

您的包裹無法送達

收件者 service@cert.tanet.edu.tw

如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

訊息 未命名的附件 00022.txt

你好，

**最後提醒：** 該電子郵件通知您的貨件仍在等待處理中。

您的包裹無法在交付 **08.04.2021** 因為沒有繳納關稅 ( **369 NT Dollars**)

**商家：中華郵政**  
**訂單號碼：00275029**  
**採購金額：369 新台幣**  
**計劃於 09.04.2021-10.04.2021** <https://www.jonkeinteriors.co.za/web.php>  
 按一下以追蹤連結

- 確認包裹的運輸 [點擊這裡](#)。

當您到達家庭住址時，您將收到一封電子郵件或短信。從可用之日起，您將有 8 天的時間撤消包裹。提款後，系統會要求您提供 ID。

- 如需更多服務，請通過以下方式查找您的貨件的後續行動 [點擊這裡](#)。

謝謝您的信任，

真摯地，  
您的中華郵政客戶服務。

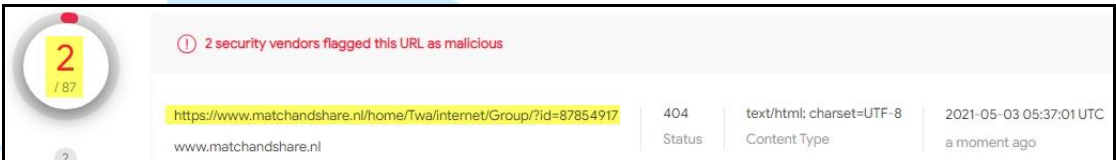
Compensation  
Chunghwa Post Co., Ltd. (hereinafter the "Company") is committed in respecting all users' personal privacy, being in accord with the Personal Information Protection Act of Republic of China and Company's personal information protection policy. The Company hereby declaring the following statements in regards with the collection, processing,



Fortinet	Phishing	SCUMWARE.org	Malware
Sophos	Phishing	ADMINUSLabs	Clean

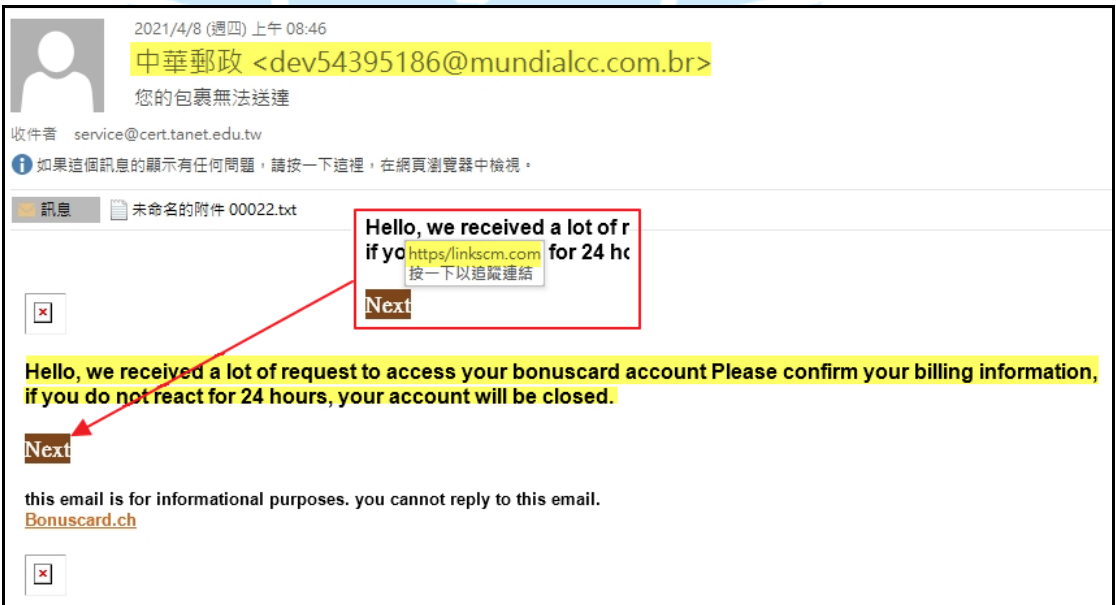
轉址的網址

「<https://www.matchandshare.nl/home/Twa/internet/Group/?id=87854917>」經 Virustotal 檢測其惡意比例為 2/87，僅兩家防毒軟體公司的防毒軟體可檢測出其為釣魚網站。



Fortinet	Phishing	Webroot	Malicious
----------	----------	---------	-----------

第 5 封信與第 6 封信的信件內容相同，僅信件最後隱藏底文的內容不同。第 5 封的底文內容請收件者在 24 小時內存取帳戶並確認帳單資訊，若超過 24 小時則帳戶將被關閉。內容中也提供一個連結網址 (<https://linkscm.com>)，但因網址的格式錯誤無法開啟網頁。



2021/4/8 (週四) 上午 08:46  
中華郵政 <dev54395186@mundialcc.com.br>  
您的包裹無法送達  
收件者: service@cert.tanet.edu.tw  
如果這個訊息的顯示有任何問題，請按一下這裡，在網頁瀏覽器中檢視。

訊息 未命名的附件 00022.txt

Hello, we received a lot of request to access your bonuscard account Please confirm your billing information, if you do not react for 24 hours, your account will be closed.

Next

this email is for informational purposes. you cannot reply to this email.  
<https://linkscm.com>

檢視第 5 封信的 MailHeader 發現該信件寄件者 IP 為來自巴西 IP:



201.76.147.11。

Summary					
<p>Subject 您的包裹無法送達  Message Id &lt;E1IUInx-000IxL-M4@srv-cpanel.hybridcc.com.br&gt;  Creation time Wed, 07 Apr 2021 21:45:53 -0300 (Delivered after 3 seconds)  From 中華郵政 &lt;dev54395186@mundialcc.com.br&gt;  To service@cert.tanet.edu.tw</p>					
Received headers					
Hop	Submitting host	Receiving host	Time	Delay	Type
1	mundialcccom	srv-cpanel.hybridcc.com.br	4/8/2021 8:45:59 AM		local (Exim 4.94) (envelope-from <mundialcccom@srv-cpanel.hybridcc.com.br>)
2	srv-cpanel.hybridcc.com.br (srv-cpanel.hybridcc.com.br [201.76.147.11])	cert.tanet.edu.tw (Postfix)	4/8/2021 8:46:02 AM	3 seconds	ESMTP

10. 由前述檢測結果可得知這 6 封信件的內容全都相同，僅中、英文版與是否有隱藏底文的差異。彙整這 6 封信件的寄件者 IP 與連結網址資訊如下表，由表中可以知道這些信件的寄件者 IP 大都來自德國，而且信中所用的連結網址都不固定。因此，這些網址在短時間內能被防毒軟體判定為惡意網址的比例很低。

信件編號	寄件者 IP	點擊網址	Virustotal	轉址網址	Virustotal
1	46.4.227.78 (德國)	http[://]pre[.]asocs[.]info/wp-maill.php	0	https[://]www[.]af raso[.]org/sites/all/new.php?id=64406665	2/87
2	81.169.211.109 (德國)	http[://]pre[.]asocs[.]info/wp-maill.php	0	https[://]www[.]af raso[.]org/sites/all/new.php?id=38476680	2/87
3	195.225.209.16 (德國) 195.158.54.3 (德國)	https[://]cursedanarchy[.]com/new.php	1/87	---	---
4	74.208.58.198 (美國) 82.165.159.134 (德國)	http[://]pixlfeed[.]com/wp-admin/user/wp.php	0	---	---
5	201.76.147.11 (巴西)	https[://]www[.]jonkeinteriors[.]co[.]za/web.php	3/87	https[://]www[.]matchandshare[.]nl/home/Twa/interne t/Group/?id=37345812	2/87

信件編號	寄件者 IP	點擊網址	Virustotal	轉址網址	Virustotal
6	rightby.store.d0m.de(192.168.44.84)(德國)	http[:]//quantum-dental[.]de/wp.php	2/87	https[:]//fmbpda[.]com/kio/Twa/internet/Group/f42cb/SSLAuthUI.html	11/87
		https[:]//administrativos[.]cl/wp.php	7/87		

### 三、攻擊行為示意圖

本案主要以第 6 封信件的檢測為主，故攻擊行為的示意圖將以第 6 封信的攻擊行為來進行說明。



1. 駭客隨機以中華郵政名義寄出主旨為「您的包裹無法送達」的釣魚郵件。
2. 收信者打開釣魚郵件。
3. 收信者被誘騙點擊信中連結網址。
4. 連結網址轉址至偽冒的信用卡付款頁面。
5. 收信者於信用卡付款頁面輸入自己的信用卡卡號與信用卡資訊來支付 369

元。

- 6.駭客透過信用卡付款頁面取得收信者的信用卡卡號與信用卡資訊。
- 7.收信者確認付款後系統請收信者進行手機簡訊之密碼驗證作業。
- 8.系統告知收信者密碼驗證失敗，並警告輸入 3 次錯誤密碼後交易會被取消，信用卡會被凍結。

#### 四、總結與建議

1. 從本案可得知駭客在郵件內容的製作上，由一開始英文版內容漸漸轉變為中文版的信件內容。雖然內容皆相同，但若收信者為可閱讀中文者則可取信於收信者。
2. 因釣魚郵件寄出一段時間後點擊的網址會被舉報為惡意網址，故駭客每批寄出的信件之點擊網址皆不同。多數信件的點擊網址會加入轉址功能，來轉址至信用卡付款頁面。
3. 從信用卡付款頁面的設計可得知駭客誘騙收信者提供信用卡卡號與信用卡資訊的網頁做的如同一般線上刷卡付款的頁面，將提高收信者的信任度。
4. 收信者在輸入信用卡卡號與信用卡資訊並點選「確認付款」按鈕後，駭客就取得收信者的信用卡卡號與信用卡資訊，推測手機簡訊之密碼驗證作業僅為取信於收信者而設計。
5. 由「系統告知密碼驗證失敗，並警告輸入 3 次錯誤密碼後交易會被取消，信用卡會被凍結」等訊息，推測此為駭客詐騙收信者要輸入正確的信用卡資訊的手法。若一直無法驗證成功，也可讓收信者誤認為交易已被取消，沒有付款成功，進而降低收信者的防備之心。
6. 從 6 封釣魚信件的寄出信件 IP 可得知這些信件大部分由德國的郵件伺服器寄出。

7. 對於預防本案的攻擊事件，有下列幾點防護措施提供參考。

- (1) 不隨意開啟不明來源的信件。
- (2) 不隨意點選(開啟)不明來源的網址(網頁)。
- (3) 當信件內容要求進行線上刷卡付款時，需特別確認寄件者的身分與刷卡網址的真實性。
- (4) 若不慎將信用卡資訊透過不明網址提供給不明人士，建議停用該信用卡，以避免信用卡被盜刷之風險。

