



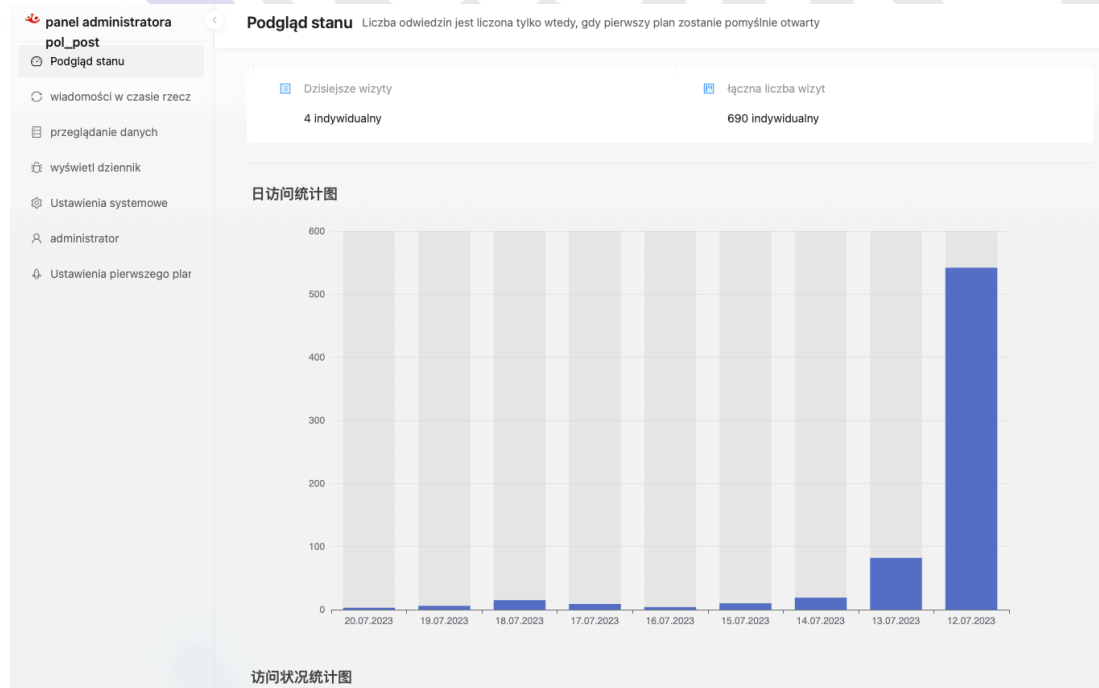
# Międzynarodowa Kampania Phishingowa Podszywająca się pod Instytucje Pocztowe: Analiza

## Wstęp:

Niniejszy raport prezentuje wyniki naszej najnowszej analizy CTI, która dotyczyła szczególnie złośliwej kampanii phishingowej skierowanej przeciwko użytkownikom tradycyjnej poczty na całym świecie. Kampania ta charakteryzowała się wyrafinowaniem i zakrojeniem na dużą skalę, a celem atakujących były takie kraje jak Polska, Boliwia, Norwegia, Portugalia, Kuwejt, Estonia i wiele innych.

Najbardziej niepokojącym aspektem tej kampanii była jej specyfika: atakujący podszywali się pod różne, zaufane instytucje pocztowe, w celu wprowadzenia użytkowników w błąd i kradzieży ich środków pieniężnych. Przestępcy przesyłali wiadomości informujące o rzekomych problemach z przesyłką, zawierające link do fałszywej strony. Użytkownicy, którzy kliknęli w link, zostali przekierowani na stronę, która wyglądała identycznie jak prawdziwa strona poczty, gdzie byli proszeni o podanie swoich danych do kart płatniczych.

Dzięki naszej analizie udało nam się jednak zidentyfikować infrastrukturę wykorzystywaną przez atakujących w tej kampanii, w tym lokalizacje serwerów, domeny i adresy IP. Co więcej, udało nam się odkryć panele administracyjne używane przez atakujących do monitorowania i zarządzania swoimi atakami. Te odkrycia umożliwiły nam głębsze zrozumienie strategii i taktyk stosowanych przez atakujących, a także zapewniły cenne informacje, które mogą pomóc w przeciwdziałaniu takim atakom w przyszłości.



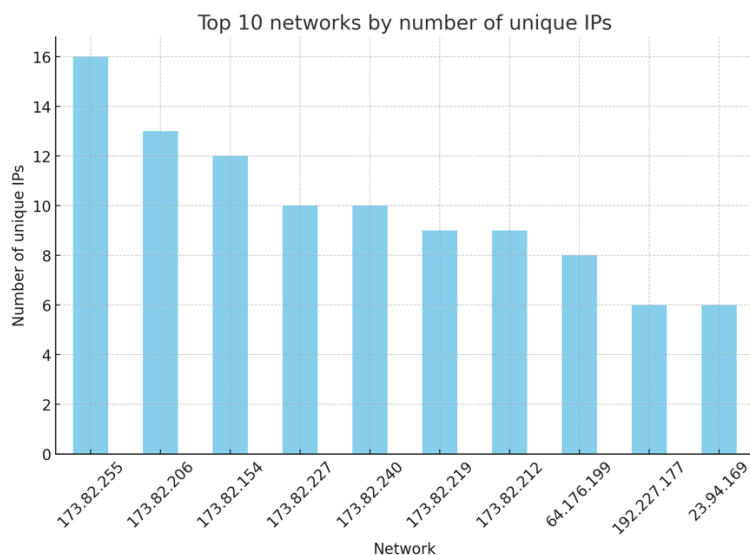
Rysunek 1 - Panel administratora kampanii phishingowej na: Poczta Polska.

## Analiza:

---

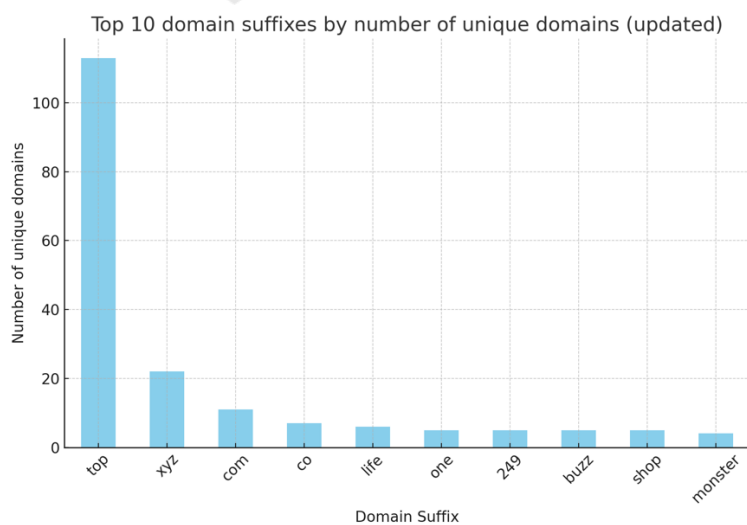
### Statystyki:

Infrastruktura wykorzystana w omawianej kampanii phishingowej była złożona i rozległa, co po raz kolejny podkreśla rozbudowany charakter tego rodzaju ataków. Atakujący korzystali z różnorodnych domen i adresów IP, co wskazuje na szeroki zasięg i skomplikowaną naturę ich działań.



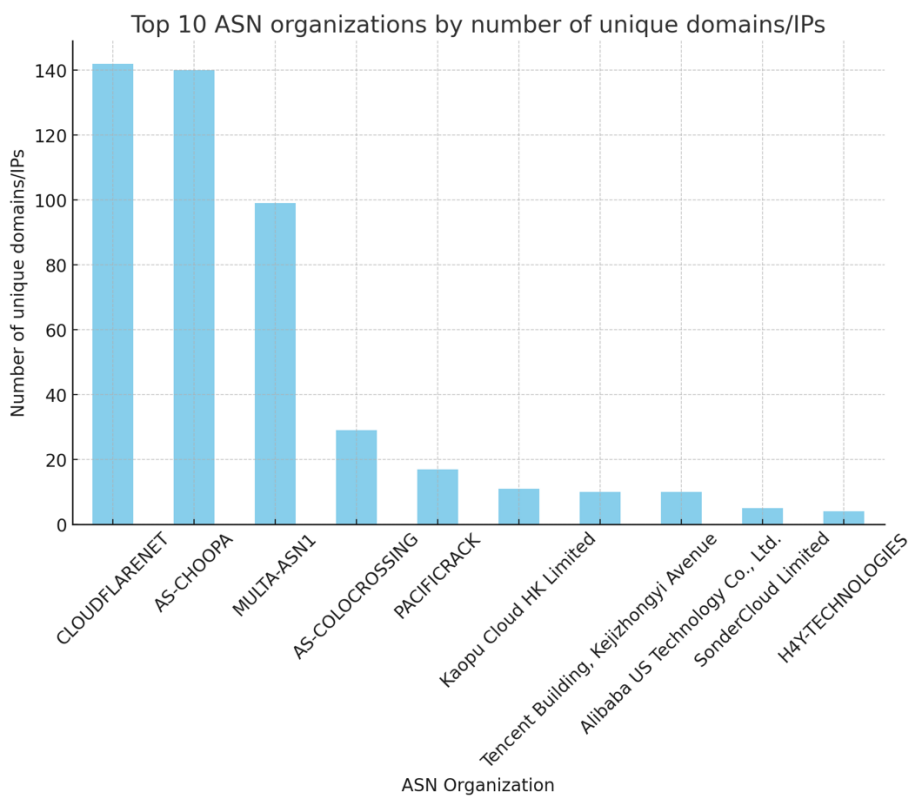
Rysunek 2 - Top 10 sieci IP wykorzystywanych w atakach.

Nasza analiza pozwoliła zidentyfikować unikalne domeny, które były wykorzystane w ramach tej kampanii. Wśród nich, szczególnie często pojawiały się domeny z sufiksami takimi jak .top, .xyz, .buzz, co może sugerować preferencje atakujących pod względem wyboru konkretnych typów domen.



Rysunek 3 - Top 10 domen wykorzystywanych w atakach.

Dodatkowo, dzięki informacjom o ASN, zdołaliśmy zidentyfikować organizacje, które były często wykorzystywane jako punkty wyjścia dla ataków. Te organizacje pochodziły z różnych krajów, co pokazuje, jak globalny był zakres tej kampanii.



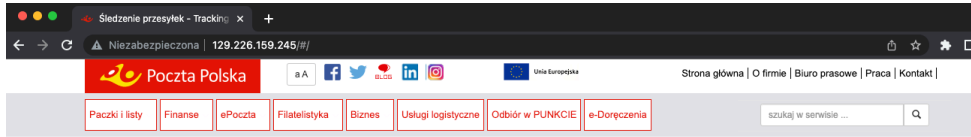
Rysunek 4 - Top 10 ASN wykorzystywanych w atakach.

## Sledzenie infrastruktury:

Adres fałszywej strony podszywającej się pod Poczte Polską: *poczta-polskad[.]top*

Adres IP: *129.226.159[.]245*

mmh3 favicon hash: *1797175259*



Strona główna > Współpraca > Sledzenie przesyłek - Tracking

### Status przesyłki

Twój numer pakietu: 856704565

**Zawiadomienie o porażce dostawy**

- Ponieważ adres dostawy nie jest jasny, pakiet nie jest dostarczany
- Twój pakiet powrócił do naszego centrum operacyjnego
- Zaktualizuj swój adres, wysłamy ponownie w 21.07.2023

[Kontynuować](#)

### Passive DNS:

- poczta-polskad[.]top
- omnivai[.]xyz
- trojan.zohocloud[.]xyz

**URL:**  
https://poczta-polskad.top

**Device type:**  
Desktop

**User agent:**  
Chrome Android

[Szukaj](#)

---

**Scanning URL:** https://poczta-polskad.top  
Adres IP: 129.226.159.245  
 Oznacz IP jako niebezpieczne

**Serwisy:**

[Shodan](#)
[GreyNoise](#)
[VirusTotal](#)
[Censys](#)
[CriminallP](#)
[URLScan](#)

**Powiązane domeny (50):**

LP.	DOMAIN	DATA AKTUALIZACJI	DATA UTWORZENIA
1.	poczta-polskad.top	2023-07-20 11:46:21	2023-07-20 09:50:18
2.	omnivai.xyz	2023-07-17 08:00:22	2023-07-15 11:04:34
3.	trojan.zohocloud.xyz	2021-11-22 11:30:38	2020-10-27 14:34:12

**FOFA.info:**

Query: ip="129.226.159.245"

No	Host/Fid	IP	Port/Protocol	Domain	Lastupdate time
1	129.226.159.245:22	129.226.159.245	22 ssh	-	2023-07-17
2	https://129.226.159.245	129.226.159.245	443 https	-	2023-07-16
3	https://129.226.159.245	129.226.159.245	443 https	-	2023-07-16
4	129.226.159.245	129.226.159.245	80 http	-	2023-07-16
5	129.226.159.245	129.226.159.245	80 http	-	2023-07-16
6	www.omnival.xyz	129.226.159.245	80 https	omnival.x	2023-07-15
7	https://www.omnival.xyz	129.226.159.245	443 https	omnival.x	2023-07-15
8	omnival.xyz	129.226.159.245	80 https	omnival.x	2023-07-15
9	https://omnival.xyz	129.226.159.245	443 https	omnival.x	2023-07-15

**FOFA.info FID:**

Query: fid="mwPk6F0j6G0YSMxscpiQbg=="

No	Host/Fid	IP	Port/Protocol	Domain	Lastupdate time
1	https://tr-ptgovtr.top	172.67.174.223	443 https	tr-ptgovtr	2023-07-20
2	https://correos-zl.net	104.21.70.151	443 https	correos-zl	2023-07-20
3	https://www.resubmito.com	173.82.206.249	443 https	resubmito	2023-07-20
4	https://www.open-rich.com	173.82.206.126	443 https	open-rich	2023-07-20
5	https://173.82.206.126	173.82.206.126	443 https	-	2023-07-20
6	https://23.94.169.116	23.94.169.116	443 https	-	2023-07-20
7	https://45.32.152.87	45.32.152.87	443 https	-	2023-07-20
8	https://georgianpost.com	23.94.169.116	443 https	georgianp	2023-07-20
9	https://israelpostoffice.com	45.32.152.87	443 https	israelpost	2023-07-20
10	https://resubmito.com	173.82.206.249	443 https	resubmito	2023-07-20

Favicon:



Zidentyfikowane oraz aktywne strony phishingowe na dzień 20.07.2023:

Korea Południowa - hxxps://epost-go-kr[.]xyz/#/

The screenshots show a phishing website designed to look like the official Korean Postal Service (우정사업본부) website. The URL is https://epost-go-kr[.]xyz/#/.

**First Screenshot:** A payment page titled "온라인 결제" (Online Payment). It informs the user that a card payment is required and provides a card number (0000 0000 0000 0000), an expiration date (MM/YY), and a security code (CVV). A "계속하다" (Continue) button is visible.

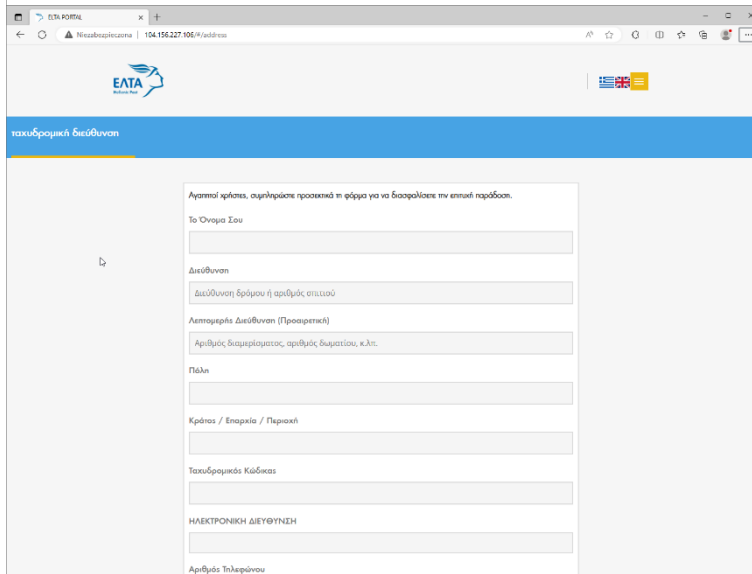
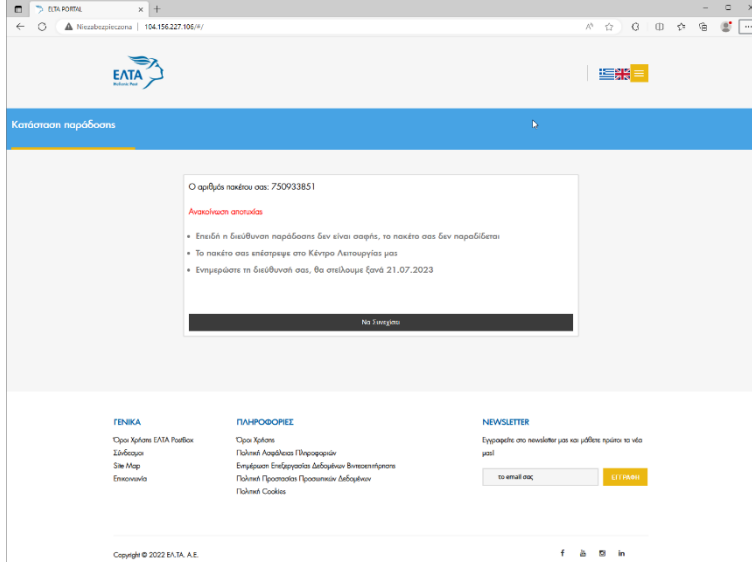
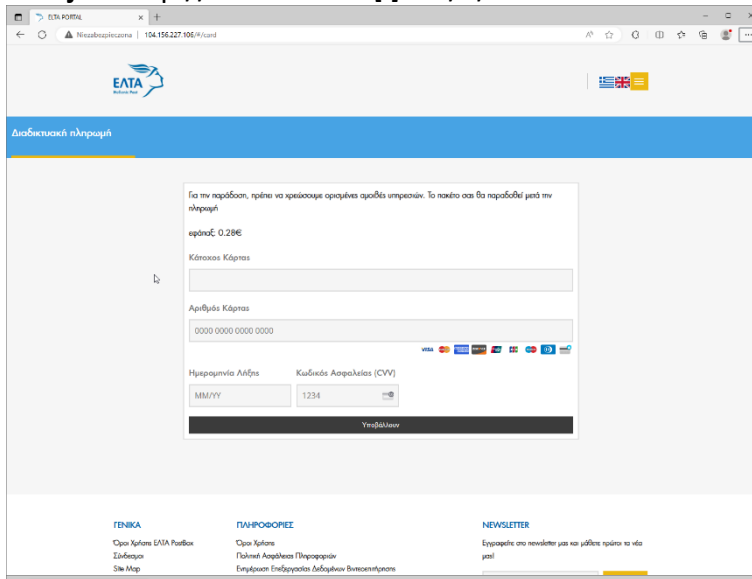
**Second Screenshot:** A "배송 상황" (Delivery Status) page. It displays a tracking number (983493976) and a "배송 실패 통지" (Delivery Failure Notification). The message states that the delivery failed because the recipient is not at home and asks the user to update their address by July 21, 2023. A "계속하다" (Continue) button is present.

**Third Screenshot:** A "우편 주소" (Postal Address) page. It prompts the user to enter their name, address, city, and phone number to complete the registration. A "즉시 업데이트하십시오" (Update Immediately) button is at the bottom.

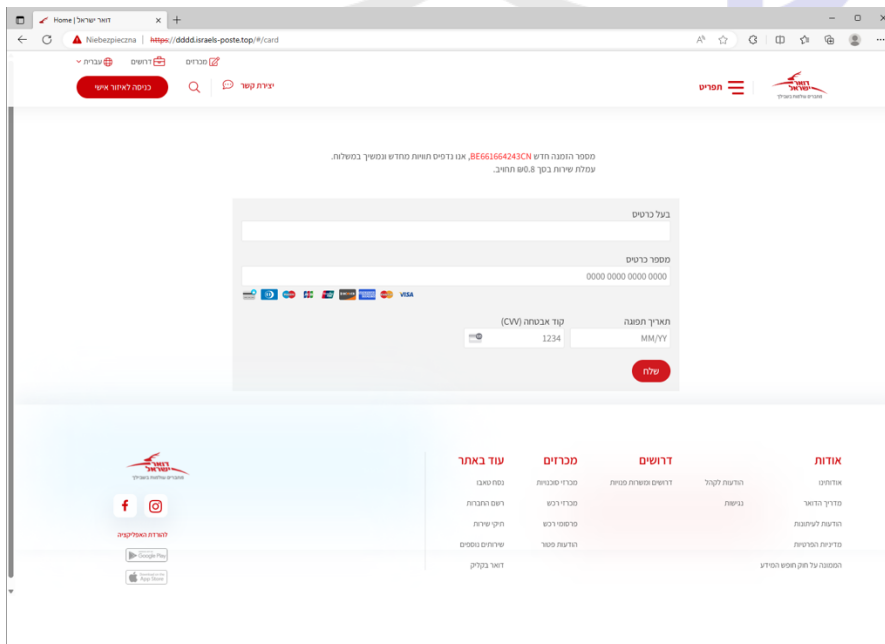
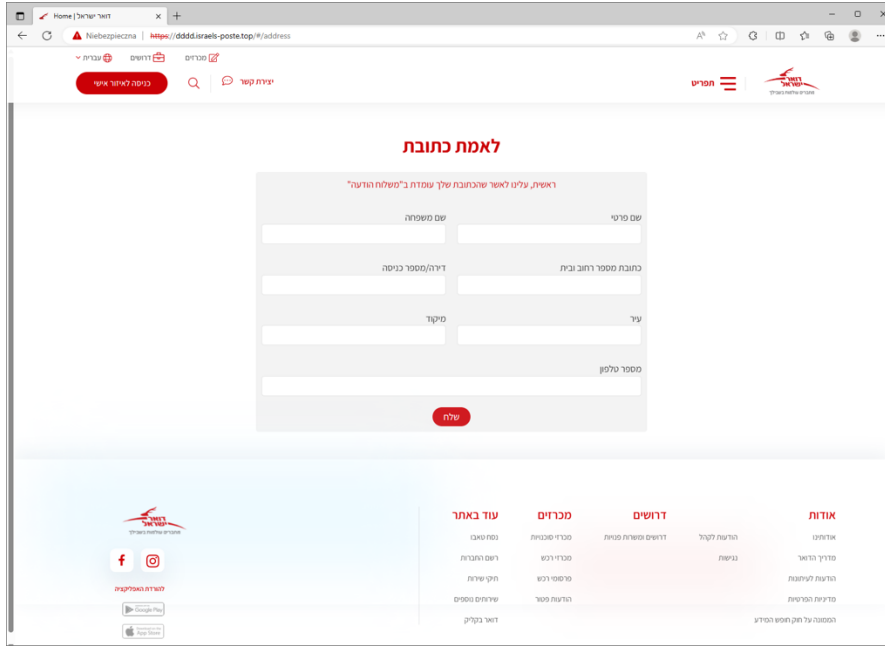




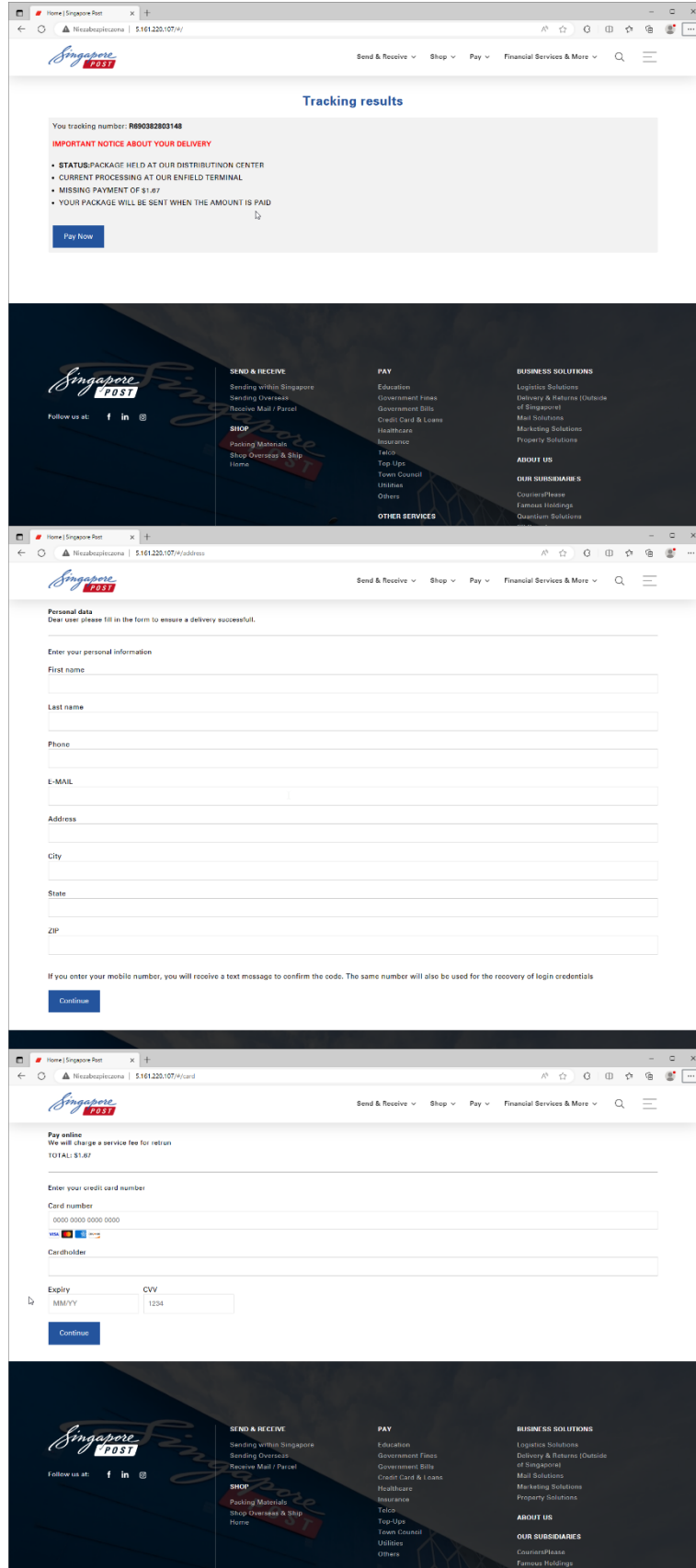
Grecja - hxxp://104.156.227[.]106/#/



### Izrael – hxxps://dddd.israels-poste[.]top/#/



Singapur - hxxp://5.161.220[.]107/#/



KNF  
IRT

# Hiszpania - hxxp://149.248.62[.]119/#/

**Estado de entrega**

Su número de paquete: 104890006

**Aviso de falla de entrega**

- Debido a que la dirección de entrega no está clara, su paquete no se entrega
- Su paquete ha regresado a nuestro centro de operaciones
- Actualice su dirección, enviaremos nuevamente en 21.07.2023

[Continuar](#)

Para ti

Para tu empresa

Para tu interés

f @ t in v

**Dirección de envío**

Estimados usuarios, complete cuidadosamente el formulario para garantizar la entrega exitosa.

Su Nombre

DIRECCIÓN: la calle o número de casa

Dirección Detallada (Opcional): no de habitación, etc.

Ciudad

Estado / Provincia / Región

Código Postal

Correo Electrónico

Número De Teléfono

[Actualizar inmediatamente](#)

**Pago en línea**

Para la entrega, necesitamos cobrar algunas tarifas de servicio. Su paquete se volverá a ceder después del pago

Suma global: 0.22€

Titular De La Tarjeta

Número De Tarjeta

Fecha De Expiración

Código De Seguridad (CVV)

[Enviar](#)

Para ti

Para tu empresa

Para tu interés

f @ t in v

Bolivia - hxxps://posta-hr[.]top/#/



**Estado de entrega**

Su número de paquete: 403167761

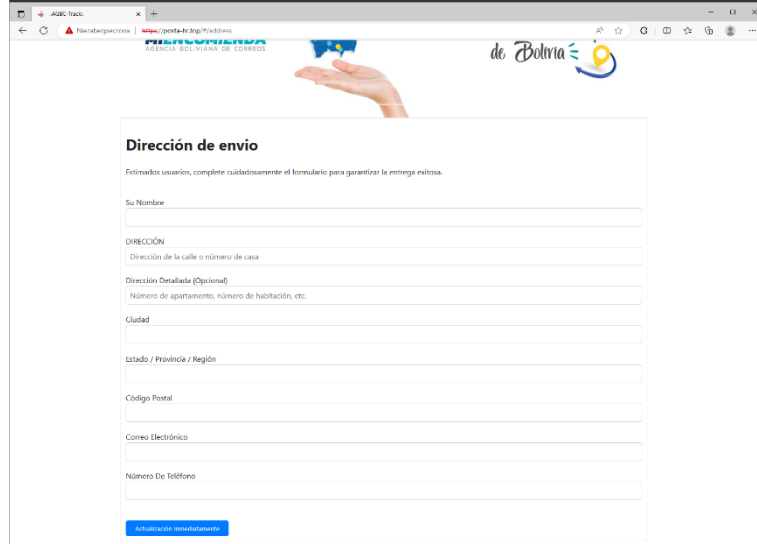
**Aviso de falla de entrega**

- Debido a que la dirección de entrega no está clara, su paquete no se entrega
- Su paquete ha regresado a nuestro centro de operaciones
- Actualice su dirección, enviaremos nuevamente en 21.07.2023

[Continuar](#)

**AGBC**

f t y



**Dirección de envío**

Estimados usuarios, complete cuidadosamente el formulario para garantizar la entrega exitosa.

Su Nombre

DIRECCIÓN

Dirección Detallada (Opcional)

Número de apartamento, número de habitación, etc.

Ciudad

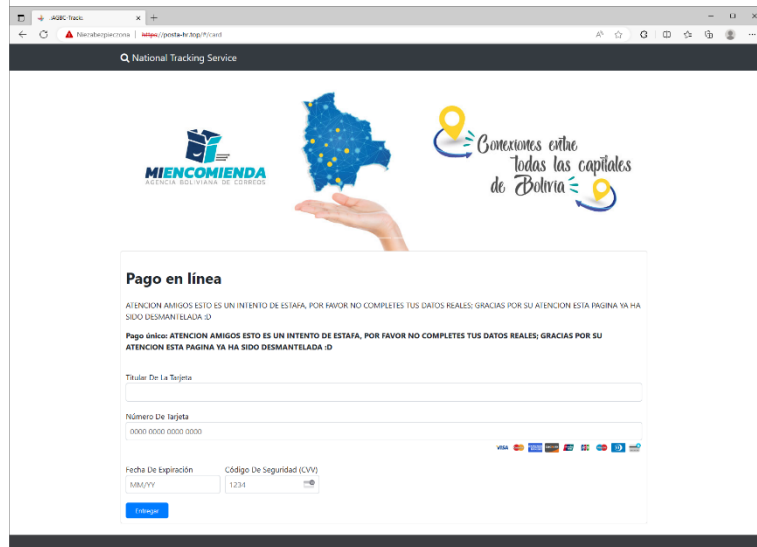
Estado / Provincia / Región

Código Postal

Correo Electrónico

Número De Teléfono

[Actualizar inmediatamente](#)



**Pago en línea**

ATENCIÓN AMIGOS: ESTO ES UN INTENTO DE ESTAFA, POR FAVOR NO COMPLETE TUS DATOS REALES; GRACIAS POR SU ATENCIÓN ESTA PAGINA VA HA SIDO DESMANTELADA -D

**Pago online: ATENCIÓN AMIGOS: ESTO ES UN INTENTO DE ESTAFA, POR FAVOR NO COMPLETE TUS DATOS REALES; GRACIAS POR SU ATENCIÓN ESTA PAGINA VA HA SIDO DESMANTELADA -D**

Titular De La Tarjeta

Número De Tarjeta

Fecha De Expiración  Código De Seguridad (CVV)

[Continuar](#)

KNF  
IRT

## DHL Niemcy - hxxp://208.85.22[.]235/#/

**Lieferstatus**

Ihre Paketnummer: 217449142

**Verzögerung bei der Lieferung**

- Da die Lieferadresse nicht klar ist, wird Ihr Paket nicht geliefert.
- Ihr Paket ist in unser Operation Center zurückgeschickt.
- Bitte aktualisieren Sie Ihre Adresse, wir werden wieder in 31.07.2023 versenden.

[Weitermachen](#)

<p><b>Privatkunden</b></p> <ul style="list-style-type: none"> <li>Preise</li> <li>Versenden</li> <li>Empfangen</li> <li>DHL Kundenkonto</li> <li>Hilfe &amp; Kontakt</li> <li>Post &amp; DHL App</li> </ul>	<p><b>Geschäftskunden</b></p> <ul style="list-style-type: none"> <li>Paket</li> <li>Express</li> <li>Logistik</li> <li>Kontakt</li> <li>Kunde werden</li> <li>DHL.com</li> </ul>	<p><b>Unternehmen</b></p> <ul style="list-style-type: none"> <li>Über uns</li> <li>DHL Group</li> <li>Karriere</li> <li>Presse</li> <li>Investoren</li> <li>Nachhaltigkeit</li> </ul>	<p><b>Wissenslager</b></p> <ul style="list-style-type: none"> <li>Stiftung</li> <li>Warentest</li> </ul>
---	--	---	--

**Social**

**Postanschrift**

Sehr geehrte Benutzer, bitte füllen Sie das Formular sorgfältig aus, um die erfolgreiche Lieferung zu gewährleisten.

Ihrer Name

Adresse

Detailierte Adresse (Optional)

Wohnungsnummer, Zimmernummer usw.

Stadt

Stadt / Provinz / Region

Postleitzahl

E-mail

Telefonnummer

[Sofort Aktualisieren](#)

**Onlinebezahlung**

Für die erneute Lieferung müssen wir einige Servicegebühren erheben. Ihr Paket wird nach Zahlungseingang erneut zugestellt.

**Pauschalbetrag: 0,18**

Kartenhalter

Kartenummer

0000 0000 0000 0000

Gültig bis  bis

OW  1234

[Einzahlen](#)

<p><b>Privatkunden</b></p> <ul style="list-style-type: none"> <li>Preise</li> <li>Versenden</li> <li>Empfangen</li> <li>DHL Kundenkonto</li> <li>Hilfe &amp; Kontakt</li> </ul>	<p><b>Geschäftskunden</b></p> <ul style="list-style-type: none"> <li>Paket</li> <li>Express</li> <li>Logistik</li> <li>Kontakt</li> <li>Kunde werden</li> </ul>	<p><b>Unternehmen</b></p> <ul style="list-style-type: none"> <li>Über uns</li> <li>DHL Group</li> <li>Karriere</li> <li>Presse</li> <li>Investoren</li> </ul>	<p><b>Wissenslager</b></p> <ul style="list-style-type: none"> <li>Stiftung</li> <li>Warentest</li> </ul>
---	---	---	--

KNF  
IRT

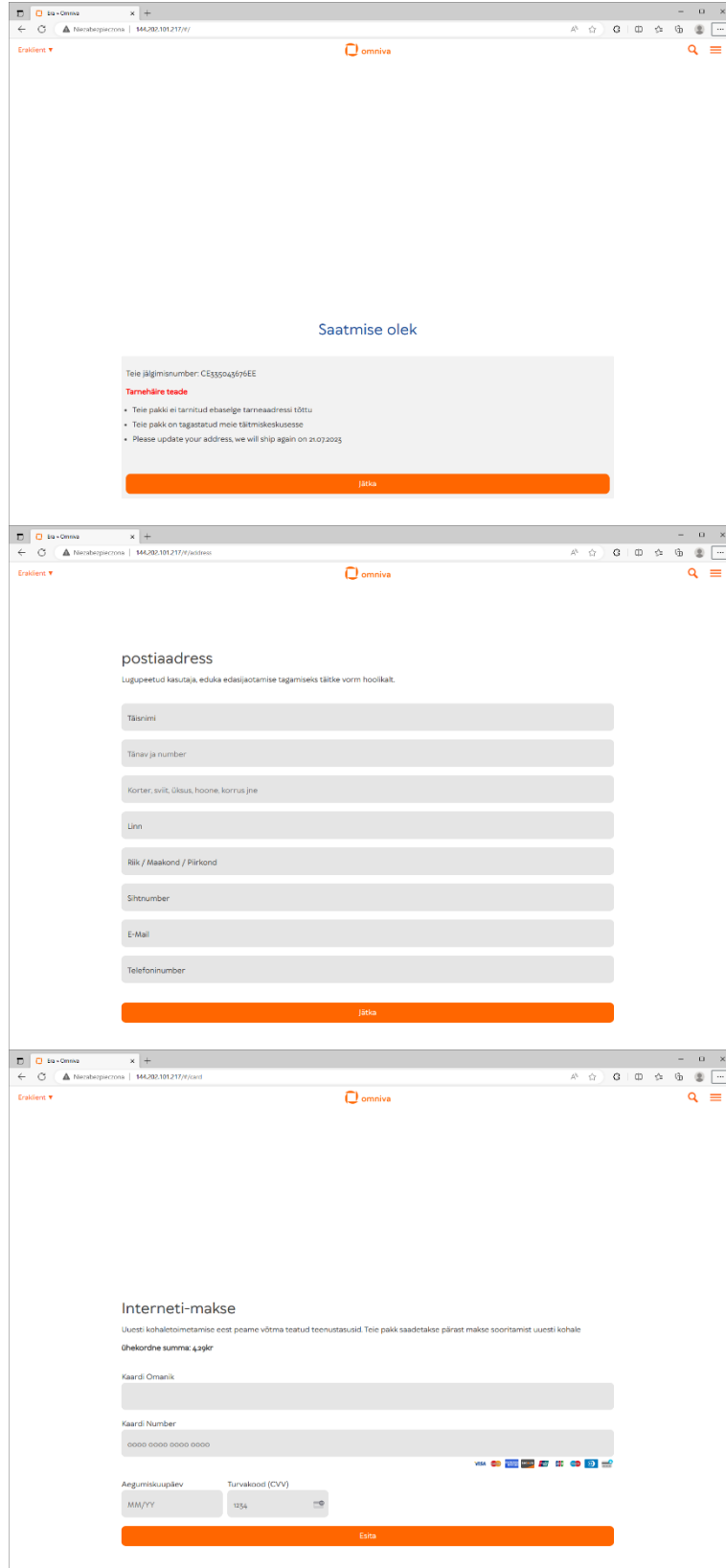


Wtochy – hxxp://64.176.189[.]221/#/

The image shows three sequential screenshots of the Posteitaliane website interface. The top screenshot displays a search for a shipment with ID XA733227828IT, which is marked as 'stato non disponibile' (not available) due to a delivery error. The middle screenshot shows the 'Dati Anagrafici' (Anagraphic Data) form, which is partially filled with placeholder text like 'insensici'. The bottom screenshot shows the 'Paga in linea' (Pay online) section, also with placeholder information. A large, semi-transparent watermark 'KNF CSIRT' is overlaid on the right side of the screenshots.



## Estonia - hxxp://144.202.101[.]217/#/



The image displays three sequential screenshots of the Omniva website interface, accessed via a browser at the URL hxxp://144.202.101[.]217/#/. The browser's address bar shows the URL and the Omniva logo is visible in the top right corner of the page.

**Top Screenshot: Saamise olek**  
The page title is "Saamise olek". It displays the tracking number: "Teie jälgimisnumber: CE532043676EE". A red heading "Tähtsähä teade" is followed by a list of items:

- Teie pakk ei tarnitud ebaselge tarneaadressi tõttu
- Teie pakk on tagastatud meie tähtsmikeskusesse
- Please update your address, we will ship again on 21.07.2023

An orange "Jätka" button is at the bottom.

**Middle Screenshot: postiaadress**  
The page title is "postiaadress". The instruction reads: "Lugupidetud kasutaja, eduka edasijäotamise tagamiseks täitke vorm hoolikalt." Below are several input fields:

- Tähtnimi
- Tänav ja number
- Korteri, süliti, üksus, hoone, korrus jne
- Linn
- Riik / Maakond / Piirkond
- Sihetnumber
- E-Mail
- Telefoninumber

An orange "Jätka" button is at the bottom.

**Bottom Screenshot: Interneti-makse**  
The page title is "Interneti-makse". The instruction reads: "Uuesti kohaletoimetamise eest peame võtma teatud teenustasusid. Teie pakk saadetakse pärast makse sooritamist uuesti kohale." Below this, it says "Ghekkordne summa: 4,39kr". There are input fields for:

- Kaardi Omanik
- Kaardi Number (with a masked value: 0000 0000 0000 0000)
- Argumntiikupälev (with a masked value: MM/YY)
- Turvakood (CVV) (with a masked value: 1234)

Payment logos for Visa, Mastercard, and others are visible. An orange "Eisa" button is at the bottom.

KNF  
IRT

## Finlandia - hxxp://66.135.28[.]18/#/

postit | Henkilölle | Yritykselle | Asiakastuki | Valittu

Paketti ja seuranta | Kirjeet ja postipalvelut | OmaPosti

### Toimituksen tila

Seurantamääritys: R062434335F1

**Toimitusvirheilmoitus**

- Pakettiasi ei toimitettu epäselvään toimitusosoitteeseen vuoksi
- Pakettiasi on palautettu toimituskeskukseemme
- Päivitä osoitteesi, lähetämme uudelleen 21.07.2023

[Jatka](#)

**Seuraa meitä**

- Facebook
- Twitter
- LinkedIn
- YouTube

**Kansainväliset sivustot**

- Latvia
- Iittua
- Skandinavia
- Viro

**Olkopolut**

- Työpaikat
- Posti yrityksenä
- Häiriöilmoitukset
- Tiedotteet
- Ota yhteyttä
- Verkkokauppa

**Lataa OmaPosti-sovellus**

Lataa App Storesta

Lataa Google Playsta

### postitusosoite

Hyvä käyttää tässä lomake huolellisesti varmistaksesi onnistuneen jakelun.

Koko nimi

Osoite

Katu ja numero

Huoneisto, silityt, yksikkö, rakennus, kerros jne

Kaupunki

Osa-alue / Maakunta / Alue

### Online Maksu

Uudelleentoimituksesi joudumme veloittamaan joltain palvelumaksua. Pakettisi toimitetaan uudelleen maksun jälkeen.

**hertakorvaus: 0,3€**

Kortin haltija

Kortin Numero

0000 0000 0000 0000

Viimeinen käyttöpäivä

Turvakoodi (CVV)

MM/YY

1234

[Lähetä](#)

KNF  
IRT

# Francja - hxxps://frpost[.]fr/#/

**Statut de livraison**

Voter numéro de package: 304489740

**Acte de livraison de défaillance**

- Parce que l'adresse de livraison n'est pas claire, votre colis a été livré
- Votre colis est retourné à notre centre d'opérations
- Veuillez mettre à jour votre adresse, nous espérons à nouveau à 21.07.2023

Continuer

**Nos Engagements**

- Proche de vous
- Priorité neutralité carbone
- Paiements 100% sécurisés
- Livraison offerte dès 21€ d'achat

Applications la Poste

Restons connectés

Nos Services, Nos Produits, Nos Tarifs, La Poste vous accompagne

**Adresse postale**

Cher utilisateur, veuillez remplir soigneusement le formulaire pour assurer la réussite de la livraison.

Votre Nom

Adresse  
Adresse de rue ou numéro de maison

Adresse D'attention  
Numéro d'appartement, numéro de chambre, etc.

Ville

Etat / Province / Région

Code Postal

E-Mail

Numéro De Téléphone

Mettre à jour l'attachement

**Paiement en ligne**

Pour une nouvelle livraison, nous devons facturer des frais de service. Votre colis vous sera livré après paiement montant forfaitaire: 0,17€

Titulaire De La Carte

Numéro De Carte  
0000 0000 0000 0000

Date D'expiration  
MM/YY

Soumettre

**Nos Engagements**

- Proche de vous
- Priorité neutralité carbone
- Paiements 100% sécurisés
- Livraison offerte dès 21€ d'achat

Applications la Poste

Restons connectés

Nos Services, Nos Produits, Nos Tarifs, La Poste vous accompagne

### Kuwejt - hxxp://208.167.242[.]249/#/

The image displays three sequential screenshots of the Kuwait Post website (www.kuwaitpost.gov.kw) in Arabic. The browser address bar shows the URL: hxxp://208.167.242[.]249/#/.

- Top Screenshot (Home):** Shows the main navigation menu with links for 'الرئيسية' (Home), 'الخدمات' (Services), 'عن بريد الكويت' (About Kuwait Post), and 'القسمة التلقائية' (Automatic Billing). A central banner features a yellow button labeled 'رابط طلب الخدمة' (Service Request Link). Below the banner, there are sections for 'كيف هي خدماتنا؟' (How are our services?), 'روابط مهمة' (Important Links), and 'خدمات البريد' (Postal Services).
- Middle Screenshot (Address Form):** Titled 'العنوان البريدي' (Postal Address), it contains a form with fields for: 'اسم' (Name), 'عنوان' (Address), 'عنوان الشارع أو رقم الشارع' (Street name or number), 'عنوان مكتب (اختياري)' (Optional office address), 'رقم التذاوير أو رقم الخدمة أو رقم التتبع' (Tracking number or service number), 'بلد' (Country), 'البريد الإلكتروني أو الهاتف' (Email or phone), 'عنوان البريد' (Postal address), 'البريد الإلكتروني' (Email), 'رقم هاتف' (Phone number), and a 'تسجيل عنواني' (Save my address) button.
- Bottom Screenshot (Online Payment):** Titled 'الدفع الإلكتروني' (Online Payment), it shows a form for entering payment details. Fields include 'مبلغ الفatura' (Invoice amount) with a value of 0.21KD, 'رقم الفatura' (Invoice number) with a value of 0000-0000-0000-0000, and 'رقم الهاتف' (Phone number) with a value of 9955. There are also fields for 'البلد' (Country) and 'الرمز البريدي' (Postal code) with values 'Ku' and '1234' respectively. A 'دفع' (Pay) button is visible.



Luxemburg - hxxp://64.176.192[.]239/#/

KNF  
IRT

Paragwaj - hxxp://155.138.129[.]182/#/

The image displays three sequential screenshots of the website for the Dirección Nacional de Correos del Paraguay (National Post Office of Paraguay). The website header includes the national coat of arms, the text 'DIRECCIÓN NACIONAL de CORREOS del PARAGUAY', 'GOBIERNO NACIONAL', and the slogan 'Paraguay de la gente'. A navigation menu is located below the header.

**First Screenshot: Rastreo de Envíos Internacionales - Estado de entrega**  
 This page shows the tracking status for a specific package. The package number is 56510736. A red warning message states: 'Aviso de falta de entrega. Debido a que la dirección de entrega no está clara, su paquete no se entrega. Su paquete ha regresado a nuestro centro de operaciones. Actualice su dirección: enviaremos nuevamente en 21.07.2023.' A green 'Continuar' button is visible at the bottom of the message box.

**Second Screenshot: Rastreo de Envíos Internacionales - Dirección de envío**  
 This page is a form for international shipping. It includes fields for: 'Su Nombre', 'DIRECCIÓN' (with a sub-note: 'Escriba en la calle o número de casa'), 'Dirección Detallada (Opcional)' (with a sub-note: 'Número de apartamento, número de habitación, etc.'), 'Ciudad', 'Estado / Provincia / Región', 'Código Postal', 'Correo Electrónico', and 'Número De Teléfono'. A green 'Validar Información' button is at the bottom.

**Third Screenshot: Rastreo de Envíos Internacionales - Pago en línea**  
 This page is for online payment. It includes a note: 'Para el envío, debemos cobrar algunas tarifas de servicio. Su paquete será enviado después del pago.' The total amount is 'Pago Único: Gs2178.83'. There is a field for 'Titular De La Tarjeta', a 'Número De Tarjeta' field (with a sub-note: '0000 0000 0000 0000'), and a 'Fecha De Expiración' field (with a sub-note: 'MM/YY'). A 'Código De Seguridad (CVV)' field is also present. A green 'Comprar' button is at the bottom. Payment logos for Visa, Mastercard, American Express, and others are shown on the right.

All three screenshots feature a footer with the coat of arms and a list of 'Enlaces de Interés' (Links of Interest) to various Paraguayan government institutions, including the Secretariat of Social Action (SAS), National Institute of Forestry (INFORNA), National Institute of Information and Communication (SICOM), National Institute of Statistics (INEC), National Institute of Indigenous Affairs (INDI), National Institute of Rural Development and Land (INIA), National Institute of Culture and Arts (INACAP), Paraguayan Institute of Indigenous Affairs (INIA), Ministry of Industry and Commerce (MIC), Ministry of Education (ME), and National Institute of Sports (INE).



Polska - https://129.226.159[.]245/#/

**Status przesyłki**

Twój numer paczki: 423201461

**Zawłodzenie o porzuce dostawy**

- Paczka została dostawiona, ale nie została odebrana przez adresata.
- Twój pakiet powrócił do naszego centrum operacyjnego.
- Zaktualizuj swój adres, wysyłając ponownie w 21.07.2023

[Kontynuuj](#)

<b>INNE USŁUGI</b> Abonamenty RTV Dział Mail eSklep Handlowi detaliczni Przesyłki specjalne Poczta tradycyjna Przesyłki pocztowe Terminizacja Usługi dla przedsiębiorców	<b>WSPÓŁPRACA</b> Logotypy Poczta Działki reklamowe Sprzedaż kradzieżowych Sprzedaż nieruchomości Wynajem nieruchomości Zaktualizuj Poczta Sprzedaż nieruchomości Własności Transport	<b>POPULARNE LINKI</b> eMarketing Cenniki Znajdź placówkę pocztową Znajdź punkt odbioru Znajdź kod pocztowy Znajdź adres pocztowy Adres prywatny Korzystaj - informacje dla Klientów Publiczne usługi Poczta Numer Adresowy (PNA) Poczta i-commerce eCommerce Komunikacja z akcjonariuszami	<b>KARIERA</b> Praca sekretarzęd Oferty pracy FAQ Pracownicze Plany Kapitałowe <b>KONTAKT</b> Kontakt Reklamacje Ochrona danych osobowych CLER1 Poczta
---	---	--	---

Poczta Polska Spółka Akcyjna, ul. Różdżańska 8, 00-940 Warszawa NIP: 525 609 73 13, KRS: 000034872 Sąd Rejonowy dla M. St. Warszawy, XII 000034872 Sąd  
 Poczta Polska S.A. (z) 7077, Wydział Krajowy Zrehabilitacji  
 Bądźmy w kontakcie!  
 801 333 444  
 (+48) 438 420 600

**adres pocztowy**

Proszę wpisać adres, aby zapewnić odbiór przesyłki

Imię i nazwisko

Adres

Adres ulicy lub numer domu

Szczegółowy adres (opcjonalnie)

Numer mieszkania, numer pokoju itp.

Miasto

Sam / Powiat / Region

Kod pocztowy

E-Mail

Numer telefonu

[Aktywacja Newslettera](#)

<b>INNE USŁUGI</b> Abonamenty RTV Dział Mail eSklep Handlowi detaliczni Przesyłki specjalne Poczta tradycyjna Przesyłki pocztowe Terminizacja Usługi dla przedsiębiorców	<b>WSPÓŁPRACA</b> Logotypy Poczta Działki reklamowe Sprzedaż kradzieżowych Sprzedaż nieruchomości Wynajem nieruchomości Zaktualizuj Poczta Sprzedaż nieruchomości Własności Transport	<b>POPULARNE LINKI</b> eMarketing Cenniki Znajdź placówkę pocztową Znajdź punkt odbioru Znajdź kod pocztowy Znajdź adres pocztowy Adres prywatny Korzystaj - informacje dla Klientów Publiczne usługi Poczta Numer Adresowy (PNA) Poczta i-commerce eCommerce Komunikacja z akcjonariuszami	<b>KARIERA</b> Praca sekretarzęd Oferty pracy FAQ Pracownicze Plany Kapitałowe <b>KONTAKT</b> Kontakt Reklamacje Ochrona danych osobowych CLER1 Poczta
---	---	--	---

**Płatność online**

W celu poprawy dostawcy możemy realizować płatności za usługi. Twój pakiet zostanie ponownie dostarczony po płatności

Wybierz: 1.21zł

Podobasz Kartę

Numer Karty

0000 0000 0000 0000

Data ważności

MM/YY

Kod Bezpieczeństwa (CVV)

1234

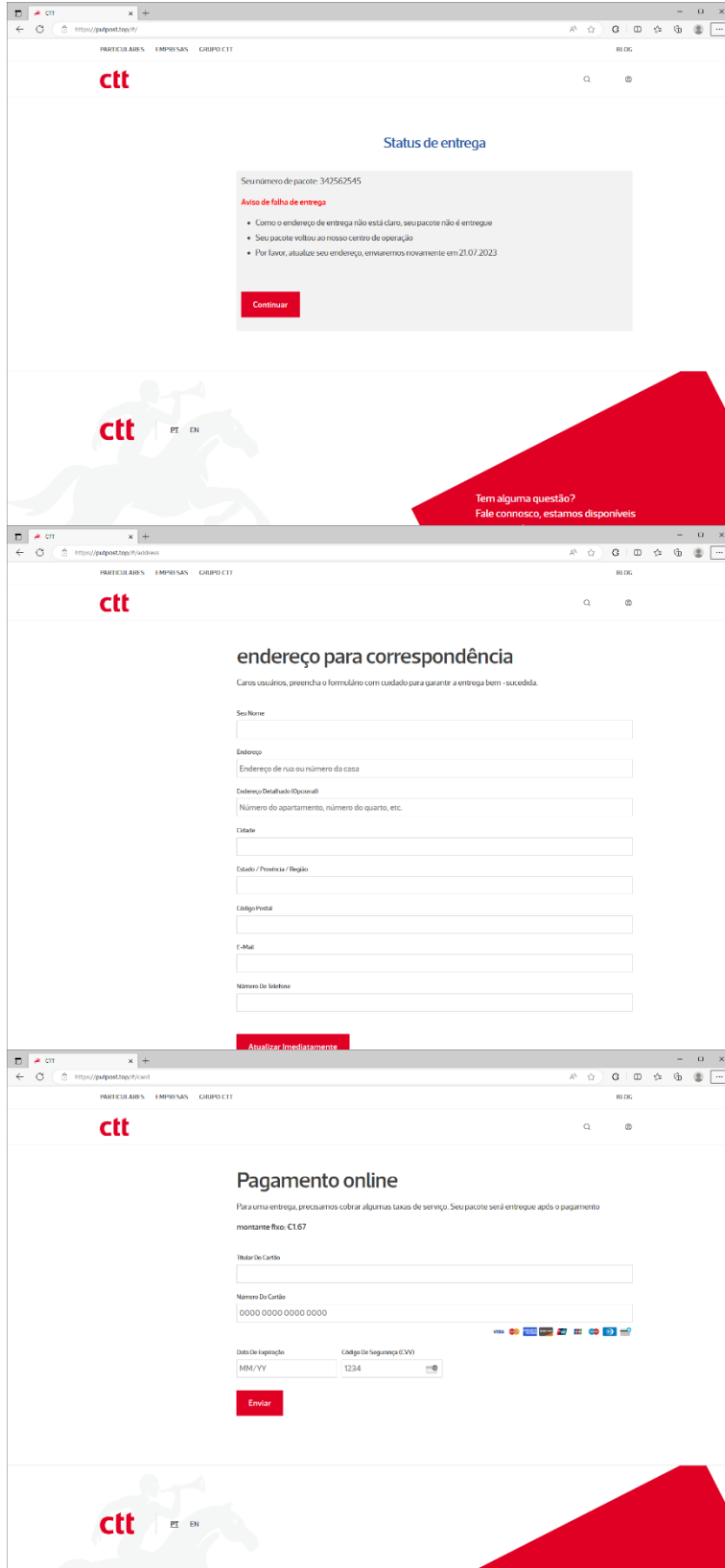
[Skasuj](#)

<b>INNE USŁUGI</b> Abonamenty RTV Dział Mail eSklep Handlowi detaliczni Przesyłki specjalne Poczta tradycyjna Przesyłki pocztowe Terminizacja Usługi dla przedsiębiorców	<b>WSPÓŁPRACA</b> Logotypy Poczta Działki reklamowe Sprzedaż kradzieżowych Sprzedaż nieruchomości Wynajem nieruchomości Zaktualizuj Poczta Sprzedaż nieruchomości Własności Transport	<b>POPULARNE LINKI</b> eMarketing Cenniki Znajdź placówkę pocztową Znajdź punkt odbioru Znajdź kod pocztowy Znajdź adres pocztowy Adres prywatny Korzystaj - informacje dla Klientów Publiczne usługi Poczta Numer Adresowy (PNA) Poczta i-commerce eCommerce Komunikacja z akcjonariuszami	<b>KARIERA</b> Praca sekretarzęd Oferty pracy FAQ Pracownicze Plany Kapitałowe <b>KONTAKT</b> Kontakt Reklamacje Ochrona danych osobowych CLER1 Poczta
---	---	--	---

Poczta Polska Spółka Akcyjna, ul. Różdżańska 8, 00-940 Warszawa NIP: 525 609 73 13, KRS: 000034872 Sąd Rejonowy dla M. St. Warszawy, XII 000034872 Sąd  
 Bądźmy w kontakcie!



### Portugalia - hxxps://www.putpost[.]top/#/



KNF  
IRT



Słowenia - hxxp://137.220.55[.]1113/#/

The image displays three sequential screenshots of the Slovenian Post website (Pošta Slovenije) in a browser window. The browser's address bar shows the URL: hxxp://137.220.55[.]1113/#/.

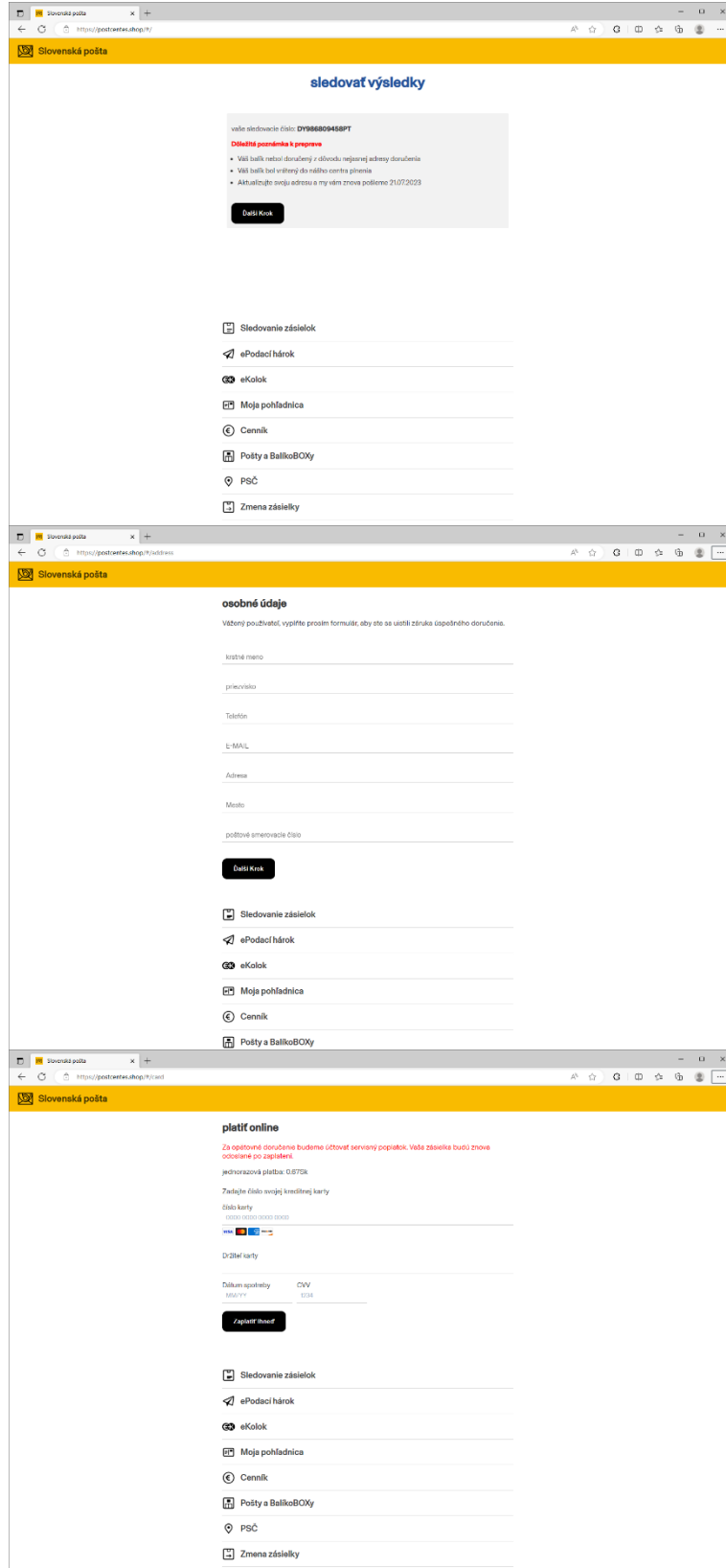
**Top Screenshot:** Shows a notification banner with the title "Vaša števila paketa: N94/26/7/368". The notification text reads: "Obravščilo o napaki o dostavi" and lists three bullet points: "Ker naša poštna dostava ni jasna, vaš paket ni dostavljen", "Vaš paket se je vmišl v naš operacijski center", and "Prosimo, posodobite svoj naslov, sicer bomo poslali v 21.07.2023". A yellow "Nadajajte" button is at the bottom.

**Middle Screenshot:** Shows the "poštni naslov" (mail address) form. The title is "Draž uporabnik, prosimo, da natančno zoponite podatke, da zagotovite uspešno dostavo." The form includes fields for: "Tvoje ime", "Nagovor", "Podroben Naslov (Neobvezno)", "Mesto", "Zvezna država / Provincias / Regija", "Poštna števila", "E-naslov", and "Telefonska številka". A yellow "Takoj Posodobite" button is at the bottom.

**Bottom Screenshot:** Shows the "Spletno plačilo" (online payment) form. The title is "Za ponovno dostavo bomo morali zaračunati nove poštnine storitve. Vaš paket bo ponovno dostavljen po operacijskem plačilu." The form includes fields for: "Imetnik Kartice", "Številka Kartice", "Rok Uporabe", and "Varnostna Koda (CVV)". A yellow "Občaj" button is at the bottom.



# Słowacja - hxxps://postcentes[.]shop/#/



## Szwecja - hxxps://postse[.]org/#/

The image displays three sequential screenshots of the PostNord website (postnord.se) in Swedish. The browser address bar shows the URL https://postse.org/#/.

- Fraktstatus:** The first screenshot shows a tracking status page for order number 230003615. It includes a "Meddelande om leveransfel" (Delivery error message) stating that the package was not delivered on time and will be re-delivered. A "Continue" button is visible.
- postadress:** The second screenshot shows the "postadress" (postal address) form. It contains several input fields for: Fullständiga Namn, Adress (gata och nummer), Lägenhet, svit, enhet, byggnad, våning, etc., Stad, Stort / Provins / Region, Postnummer, E-Mail, and Telefonnummer. A "Continue" button is at the bottom.
- Online betalning:** The third screenshot shows the "Online betalning" (online payment) page. It includes a "Kortbete" (card payment) section with fields for "Kortnummer" (0000 0000 0000 0000) and "Utgångsdatum" (MM/YY). A "Säkerhetskod (CVV)" field contains the value 1234. A "Säcker in" (Secure) button is present.

Each screenshot also shows a navigation menu at the bottom with categories: Hitta oss, Privat, Företag, Kundservice, and Om oss.

KNF  
IRT

### Turcja - hxxps://45.76.142[.]32/#/

The image shows three stacked screenshots of a web application for the Turkish Post (PTT). The browser address bar shows the URL `hxxps://45.76.142.32/#/`. The website has a yellow header with navigation links: "Posta Hizmetleri", "Tebligat", "Targif", "Kayit Elektronik Posta", "Pul ve Rakat", and "Diğer Posta İşlemleri".

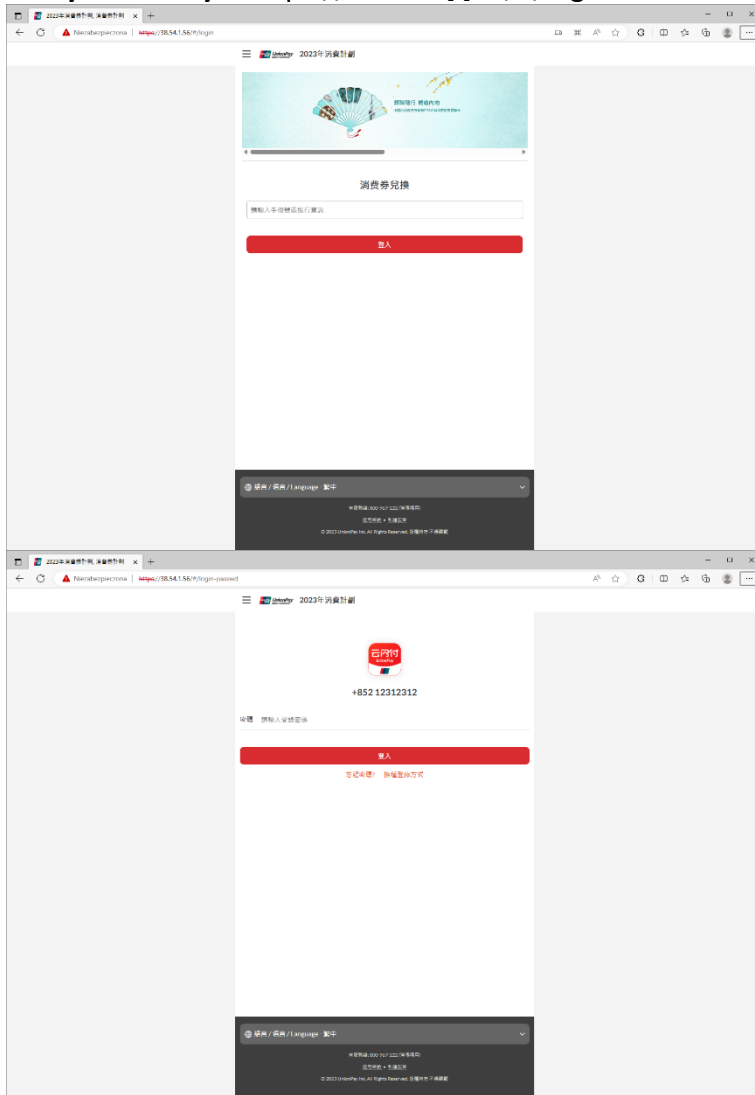
The first screenshot displays the "Teslim durumu" (Delivery Status) page for a package with number "011301965". It indicates the package is "Teslimat başlandı" (Delivery started) and lists details: "Teslimat adresi henüz onaylanmadı, paketlenmiş teslim edilemez" (Delivery address not yet confirmed, cannot be delivered packaged), "Paketiniz Operasyon Merkezi'ne döndü" (Your package returned to the Operations Center), and "Lütfen adresinizi güncelleyin, 21.07.2023'de tekrar gönderilecektir" (Please update your address, it will be re-sent on 21.07.2023). A "Detaylı Gör" (View Details) button is present.

The second screenshot shows the "posta adresi" (postal address) form. It includes fields for "Adınız", "Adres", "Ayrıntılı Adres (Bölge - Bölge)", "Şehir", "Eyalet / İl / Bölge", "Posta Kodu", "E-Posta", and "İletişim Numarası". A "Hemen Gözetile" (View Now) button is at the bottom.

The third screenshot shows the "Online ödeme" (Online payment) section. It states "Hesabın dağıtım için bakiye kontrolü yapılmıştır. Faturanız ödeme sonrası yeniden teslim edilecektir" (Your account has been checked for distribution balance. Your invoice will be re-delivered after payment). The "Kart ile online ödeme: 7.825" (Online payment with card: 7.825) is shown. There are input fields for "Kart Sıra No", "Kart Numarası", and "Banka Kullanma Tarihi". A "Gözetile" (View) button is at the bottom.

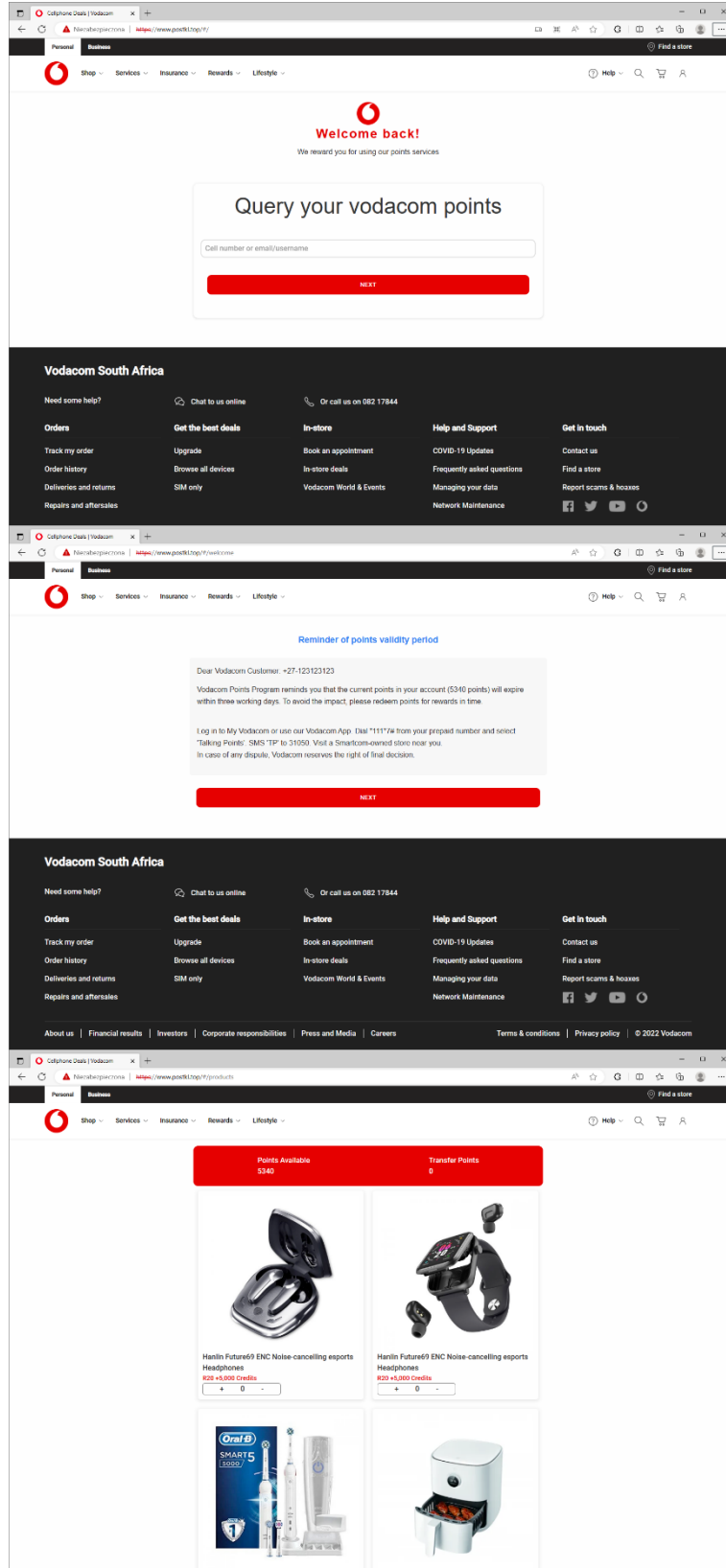


### Chiny UnionPay - hxxps://38.54.1[.]56/#/login

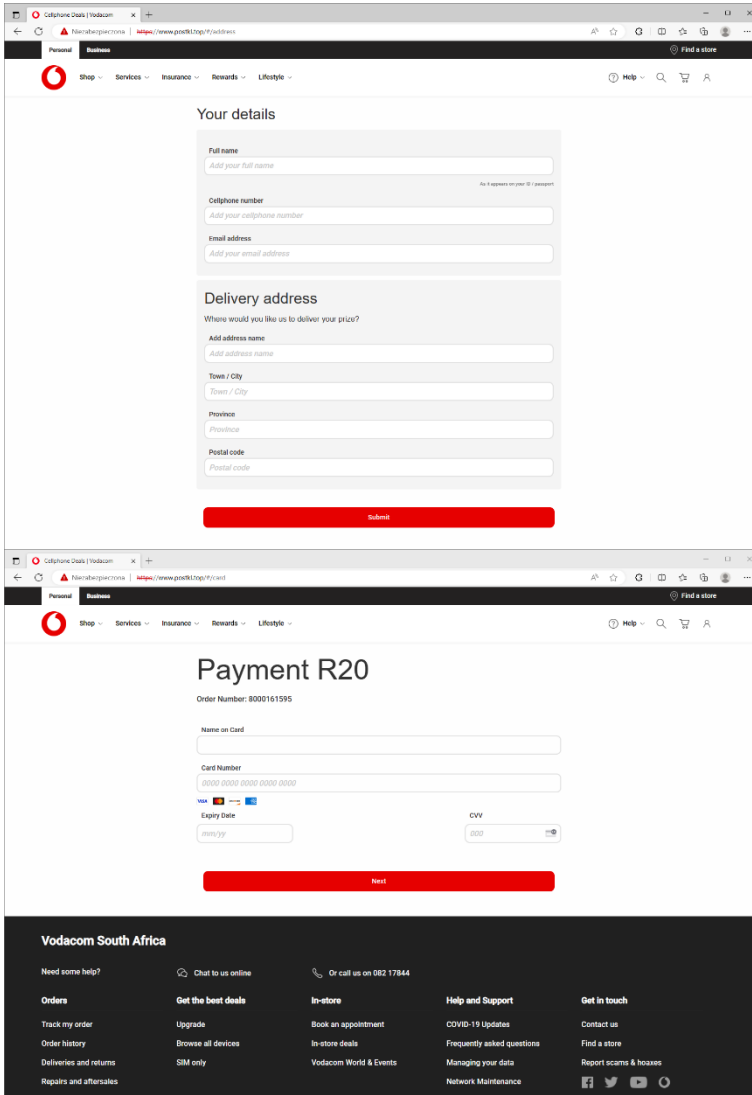


KNF  
IRT

RPA - hxxps://www.postkl[.]top/#/



KNF  
IRT



C2

Adresy IP:

'103.151.111.118',
'103.98.214.162',
'104.129.12.121',
'104.129.5.252',
'104.156.227.106',
'104.156.246.190',
'104.156.249.2',
'104.156.251.78',
'104.156.253.227',
'104.207.128.120',
'104.223.16.73',
'104.238.133.120',
'104.255.175.208',
'104.255.175.222',
'108.61.160.52',
'108.61.33.78',
'114.134.188.253',
'124.223.176.9',
'129.226.159.245',
'137.220.55.113',
'139.180.164.37',
'139.84.226.125',
'139.84.226.99',
'139.84.227.159',
'139.84.233.210',
'139.84.233.31',
'140.82.0.152',
'140.82.30.209',
'140.82.8.101',
'141.164.61.184',
'144.202.0.28',
'144.202.101.217',
'144.202.103.83',
'144.202.114.215',
'144.202.125.124',
'144.202.3.244',
'144.202.4.59',
'144.202.83.235',
'149.248.19.0',

'149.248.62.119',
'149.28.201.221',
'149.28.208.111',
'149.28.226.35',
'149.28.38.126',
'149.28.38.249',
'149.28.43.195',
'149.28.62.146',
'149.28.63.46',
'149.28.71.13',
'149.28.84.225',
'149.28.88.157',
'154.83.13.111',
'154.91.90.199',
'155.138.129.182',
'155.138.139.69',
'155.94.134.184',
'155.94.158.177',
'155.94.177.157',
'155.94.184.138',
'155.94.184.6',
'156.247.14.118',
'156.247.14.86',
'173.82.154.157',
'173.82.154.186',
'173.82.154.189',
'173.82.154.31',
'173.82.154.36',
'173.82.154.72',
'173.82.206.126',
'173.82.206.137',
'173.82.206.196',
'173.82.206.197',
'173.82.206.235',
'173.82.206.249',
'173.82.206.3',
'173.82.206.56',
'173.82.212.178',
'173.82.212.186',



'173.82.212.214',
'173.82.212.215',
'173.82.212.222',
'173.82.212.235',
'173.82.212.252',
'173.82.219.159',
'173.82.219.165',
'173.82.219.213',
'173.82.219.3',
'173.82.219.77',
'173.82.227.117',
'173.82.227.33',
'173.82.232.105',
'173.82.232.212',
'173.82.232.60',
'173.82.235.173',
'173.82.235.191',
'173.82.235.245',
'173.82.240.112',
'173.82.240.130',
'173.82.240.146',
'173.82.240.50',
'173.82.240.87',
'173.82.245.184',
'173.82.245.51',
'173.82.255.152',
'173.82.255.164',
'173.82.255.166',
'173.82.255.167',
'173.82.255.19',
'173.82.255.249',
'173.82.255.43',
'173.82.255.72',
'173.82.255.93',
'192.161.56.19',
'192.227.177.161',
'192.227.177.177',
'192.227.177.179',
'192.227.190.110',
'192.227.190.157',
'195.58.48.175',
'195.58.49.180',
'195.58.49.48',
'198.148.118.153',

'198.148.118.175',
'198.23.174.146',
'198.55.102.75',
'198.55.106.95',
'198.55.122.45',
'204.152.210.108',
'204.44.108.203',
'204.44.108.223',
'204.44.108.224',
'204.44.85.69',
'207.148.28.224',
'207.148.28.49',
'207.246.102.100',
'207.246.105.140',
'207.246.112.85',
'207.246.124.250',
'207.246.126.63',
'207.246.65.116',
'207.246.80.243',
'207.246.94.203',
'207.246.99.46',
'208.167.242.249',
'208.83.236.51',
'208.85.19.234',
'208.85.20.150',
'208.85.22.235',
'208.85.23.97',
'23.94.169.116',
'23.94.169.14',
'23.94.169.144',
'23.94.197.141',
'23.94.199.14',
'23.94.207.106',
'23.94.207.108',
'23.94.207.144',
'23.95.173.174',
'23.95.233.133',
'34.90.241.250',
'38.54.1.56',
'38.54.24.11',
'38.54.27.114',
'38.54.63.125',
'38.54.63.216',
'38.54.94.67',

'38.54.94.83',
'38.60.204.95',
'38.60.216.212',
'38.60.249.15',
'43.130.48.56',
'43.135.178.182',
'43.153.12.103',
'43.157.38.106',
'43.157.39.165',
'45.32.152.87',
'45.32.22.197',
'45.32.55.238',
'45.32.72.244',
'45.32.83.223',
'45.63.14.93',
'45.63.20.123',
'45.63.68.189',
'45.63.71.196',
'45.63.79.223',
'45.63.9.215',
'45.76.13.100',
'45.76.13.243',
'45.76.142.32',
'45.76.2.233',
'45.76.21.156',
'45.76.231.238',
'45.76.253.142',
'45.76.5.187',
'45.76.67.10',
'45.76.70.249',
'45.77.115.221',
'45.77.121.135',
'45.77.158.114',
'45.77.159.65',
'45.77.165.177',
'45.77.165.36',
'45.77.189.75',
'45.77.193.130',
'45.77.194.130',
'45.77.201.71',
'45.77.204.98',
'47.251.16.77',
'47.251.17.155',

'47.254.42.42',
'47.88.106.114',
'47.89.195.232',
'47.89.213.32',
'47.91.67.82',
'5.161.220.107',
'64.112.43.162',
'64.112.43.202',
'64.176.189.221',
'64.176.192.239',
'64.176.192.45',
'64.176.194.62',
'64.176.198.134',
'64.176.199.164',
'64.176.199.196',
'64.176.199.198',
'64.176.199.201',
'64.176.199.205',
'64.176.199.216',
'64.176.199.225',
'64.176.51.66',
'65.20.96.205',
'66.135.10.5',
'66.135.11.84',
'66.135.12.242',
'66.135.13.93',
'66.135.15.90',
'66.135.17.176',
'66.135.18.112',
'66.135.21.194',
'66.135.23.137',
'66.135.25.163',
'66.135.28.18',
'66.135.29.131',
'66.135.29.53',
'66.135.5.56',
'66.135.7.245',
'66.42.105.67',
'66.42.107.46',
'66.42.127.93',
'67.219.97.186',
'95.179.224.112'

**Domeny:**

'an-post.xyz',
'anpost-track.top',
'atpost.pro',
'ausposts.net',
'autopase.top',
'autopass-no.cc',
'autopass.bio',
'autopassno-top.top',
'autopassno.top',
'avantrawr.shop',
'bahrainpost.top',
'bpost-be.top',
'bpost.vip',
'ceskaposta.top',
'chl-correos.top',
'chl-pose-server.top',
'chl-poster-track.top',
'chl-postese-track.top',
'chl-postets-track.top',
'chl-postse-track.top',
'coles--au.shop',
'coles-au.co',
'coleş.com',
'correo.monster',
'correos-cl.cc',
'correos-cl.services',
'correos-cr.top',
'correos-es.mom',
'correos-help.xyz',
'correos-poster.xyz',
'correos-zl.net',
'correos.boats',
'correos.pics',
'correos.wang',
'correosbolivia.top',
'correosccc.top',
'correoscl.buzz',
'correosclo.top',
'correosgob.buzz',
'correogocr.co',
'correoso.top',
'correoss.online',

'cri-poste-server.top',
'cri-poster-track.top',
'cypruspost-post.services',
'de-posts-dhl.top',
'dhighpu.xyz',
'dpd-hu.top',
'e1t5bpf2.com',
'eeporstee.com',
'eeposte.net',
'elta-help.top',
'elta-new.top',
'elta-news.top',
'elta-post.top',
'eltagr.monster',
'eltagr.one',
'eltagr.top',
'enposta.top',
'epost-go-kr.xyz',
'etc-jp-nexco-etc.top',
'foodnew.top',
'foodpandatw.top',
'frpost.fr',
'georgianpost.top',
'govuk.top',
'grupoice.vip',
'hellotoby.top',
'hk-shell.top',
'hrpost.co',
'ias516fb.com',
'idme.red',
'instanthq.com',
'israeipost.top',
'israel-posts.top',
'israele-posts.top',
'israelp-post.top',
'israelpostoffice.top',
'israels-poste.top',
'jordanpost.top',
'kaz-kazpster.top',
'kddi-au.top',
'krtopaes.top',
'krtopasoet.top',

'krtopeote-track.top',
'krtopessoe-track.top',
'kuwaitpost.top',
'luhg8p7a.com',
'moc-gov.world',
'nfipz.top',
'norddk.com',
'norwaypass.co',
'nrod.top',
'omniva.top',
'omnivaee.top',
'omnivaee.xyz',
'omnivai.xyz',
'open-rice-serice.top',
'open-rich.top',
'package-tracking.top',
'plpsc.top',
'poczta-polska.one',
'polskapl.top',
'posindonesia.top',
'posnaf.top',
'post-ag.live',
'post-at.art',
'post-en.top',
'post-hr.top',
'post-news.top',
'post-office.life',
'post-server.top',
'post-t.ink',
'post-t.wiki',
'post-track-at.top',
'posta-hr.co',
'posta-hr.top',
'posta-hu.xyz',
'posta-romana.vip',
'posta-server.top',
'posta-service.top',
'posta-tracking.top',
'posta.cyou',
'posta.wang',
'postag.ws',
'postahr.buzz',
'postahu.top',
'postalparcel.info',

'postask.buzz',
'postasw.xyz',
'postcentes.cyou',
'postcentes.icu',
'postcentes.shop',
'postcentes.xyz',
'postcentres.cloud',
'postcentres.pw',
'postcentres.shop',
'postcolombia.co',
'postcorihu.top',
'postcorihu.xyz',
'poste-at.top',
'poste-it.services',
'poste-server.top',
'poste-track.top',
'poste-tracking.top',
'poste-tracks.top',
'postea-si.top',
'postea-track.top',
'poster-track.xyz',
'postifi.life',
'postifi.top',
'postkl.top',
'postlu.life',
'postnl.cyou',
'postnord-se.xyz',
'postnord.store',
'postnorddk-top.top',
'postof.top',
'postoffice-za.club',
'postoffice.lol',
'postofficeco.one',
'postpy.io',
'posts.cyou',
'postse.org',
'postslovakia.co',
'postta.top',
'postta.xyz',
'pposte-it.xyz',
'pptchek.top',
'psza.life',
'ptt-govtr.com',
'ptt-tr.top',

'ptt.monster',
'pttgovtr.top',
'putpost.top',
'qantaspoints.top',
'resubmito.top',
'scsmhd.com',
'se-postnord.top',
'se-sond.top',
'se-sond.xyz',
'se.postnord.top',
'sgphlpp.com',
'shoppee-verify-login.com',
'shoppeetw.co',
'skpost.shop',
'softbank-payment.com',
'son.postnord.top',
'sonpostnord.se',
'startselects.com',
'streamliner.co',
'sudapost.sd',
'suisseposte.top',
'swisspostpostch.buzz',
'ti-post.co',
'ti-post.top',
'tr-post.xyz',
'traveloka.cyou',
'traveloka.vip',
'tt-posts-track.top',
'ukrposhta.buzz',
'ukrposhta.vip',
'ukrposhta.world',
'ups-us.xyz',
'waws.top',
'wwwpostnordse.top',
'xn--80a7a.com',
'xn--b1alh8a.xn--p1ai',
'xn--b1av.xn--p1ai',
'xn--b1av.xn--80a7a.com',
'xn--d1abj.com',
'xn--d1abj.xn--p1ai',
'xn--d1abj1a.com',
'xn--d1abj1a.xn--p1ai',
'xn--e1akcn.com',
'xn--e1akcn.xn--p1ai',

'xn--k1afg.com',
'xn--k1afg.xn--p1ai',
'xn--k1afg1a.com',
'xn--k1afg1a.xn--p1ai',
'xn--l1adba.xn--p1ai',
'xn--m1aag.com',
'xn--m1aag.xn--p1ai',
'xn--m1adg.com',
'xn--m1adg.xn--p1ai',
'xn--p1ai.xn--80a7a.com',
'xn--p1ai.xn--b1alh8a.xn--p1ai',
'xn--p1ai.xn--b1av.xn--p1ai',
'xn--p1ai.xn--d1abj.com',
'xn--p1ai.xn--d1abj.xn--p1ai',
'xn--p1ai.xn--d1abj1a.com',
'xn--p1ai.xn--d1abj1a.xn--p1ai',
'xn--p1ai.xn--e1akcn.com',
'xn--p1ai.xn--e1akcn.xn--p1ai',
'xn--p1ai.xn--k1afg.com',
'xn--p1ai.xn--k1afg.xn--p1ai',
'xn--p1ai.xn--k1afg1a.com',
'xn--p1ai.xn--k1afg1a.xn--p1ai',
'xn--p1ai.xn--l1adba.xn--p1ai',
'xn--p1ai.xn--m1aag.com',
'xn--p1ai.xn--m1aag.xn--p1ai',
'xn--p1ai.xn--m1adg.com',
'xn--p1ai.xn--m1adg.xn--p1ai',
'yemenpost.top',
'za-post.top',
'za-poste.xyz',
'za-postoffice.xyz',
'za-postserve.xyz'