TLP:CLEAR

MIĘDZYNARODOWA KAMPANIA PHISHINGOWA ANALIZA

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

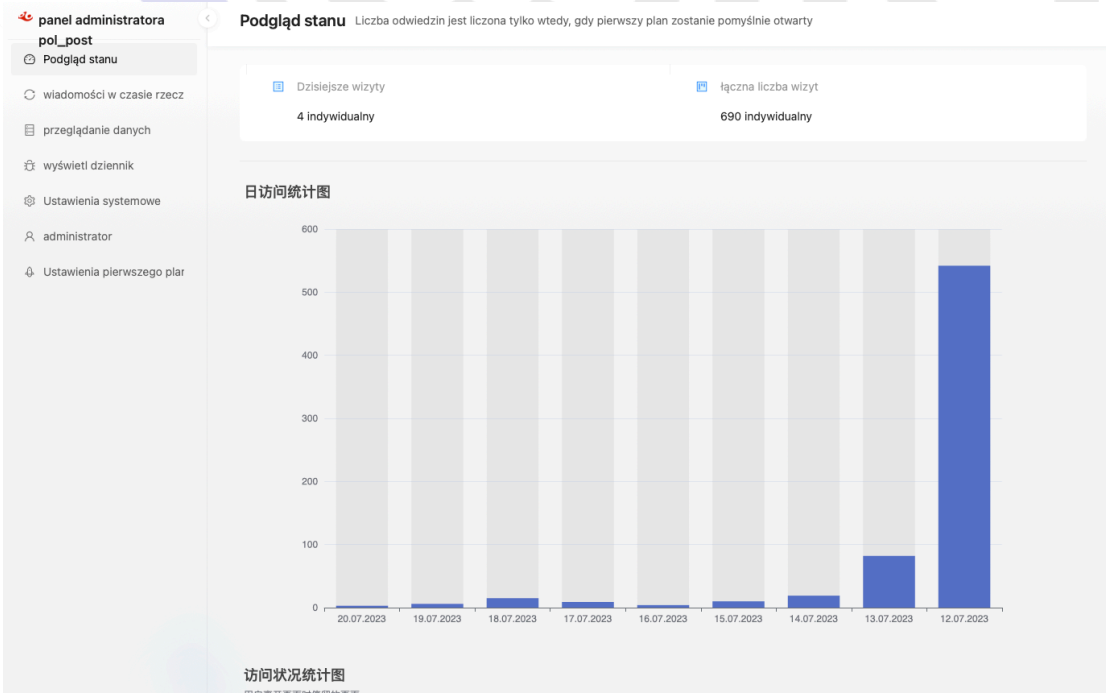
Międzynarodowa Kampania Phishingowa Podszywająca się pod Instytucje Pocztowe: Analiza

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.

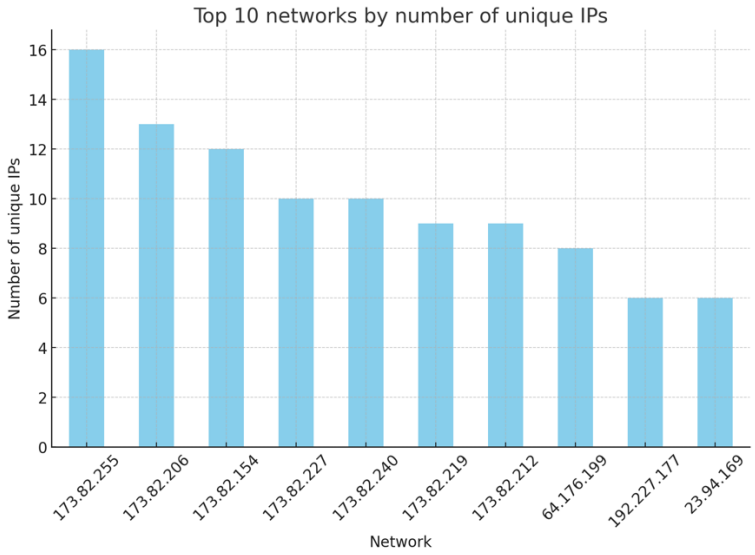


Rysunek 1 - Panel administratora kampanii phishingowej na: Poczta Polska.

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

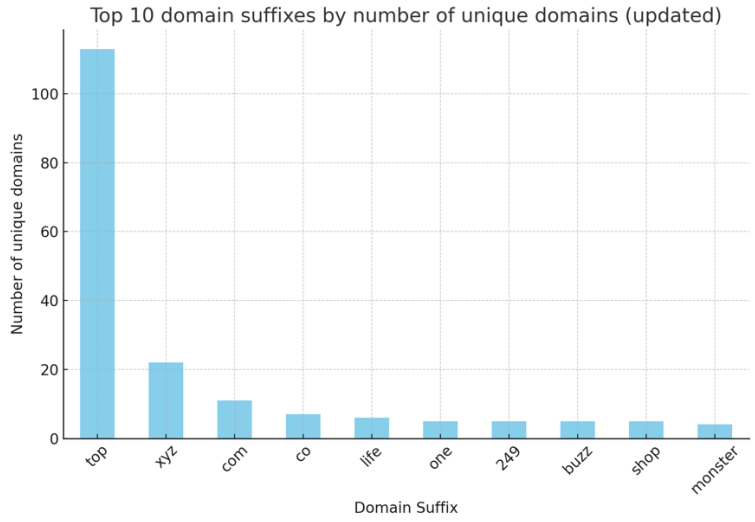
Analiza:

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.

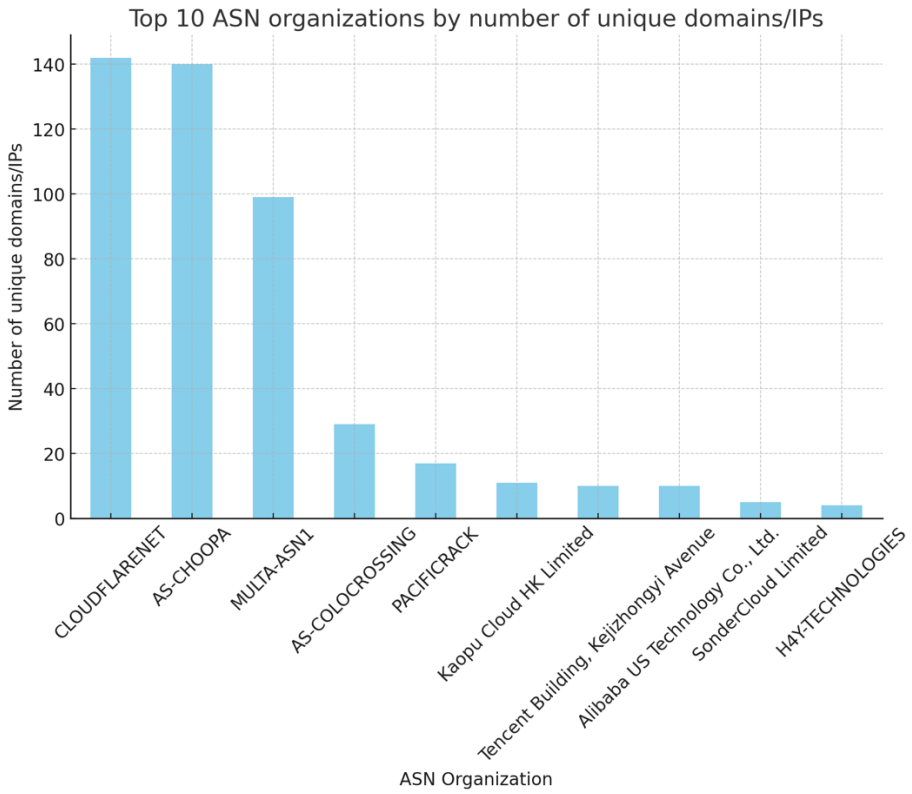
Nasza analiza pozwoliła zidentyfikować unikalne domeny, które były wykorzystane w ramach tej kampanii. Wśród nich, szczególnie często pojawiały się domeny z sufiksami takimi jak .top, .xyz, .buzz, co może sugerować preferencje atakujących pod względem wyboru konkretnych typów domen.



Rysunek 3 - Top 10 domen wykorzystywanych w atakach.

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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.

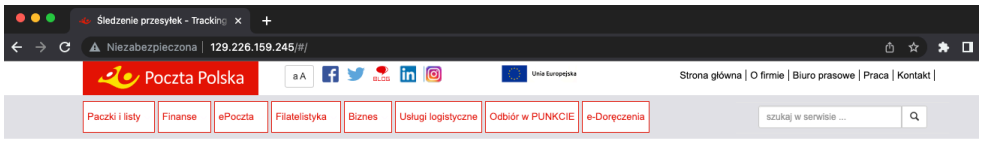


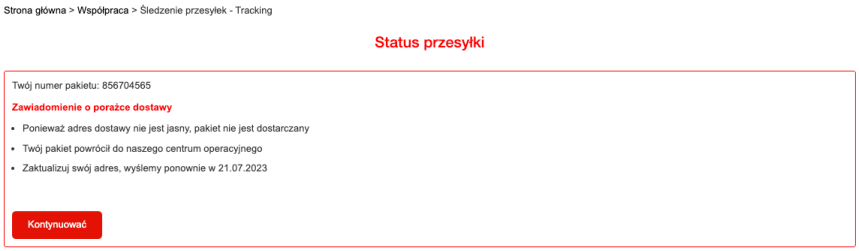
Rysunek 4 - Top 10 ASN wykorzystywanych w atakach.

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

Śledzenie infrastruktury:

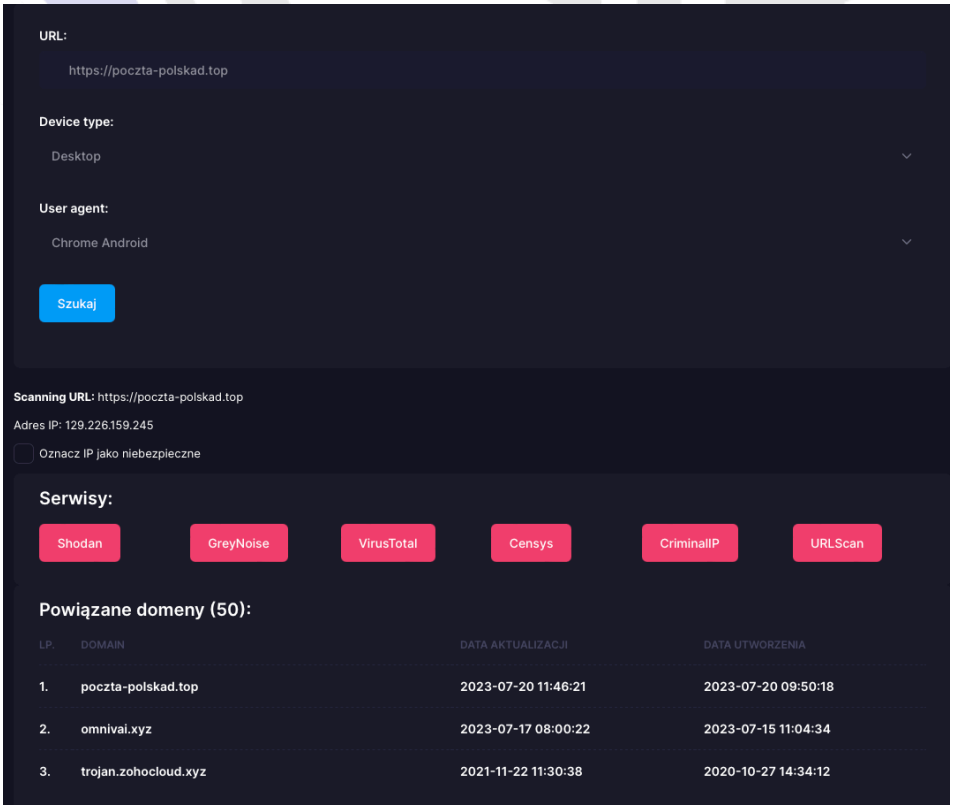
Adres fałszywej strony podszywającej się pod Pocztę Polską: *poczta-polskad[.]top*
Adres IP: *129.226.159[.]245*
mmh3 favicon hash: *1797175259*





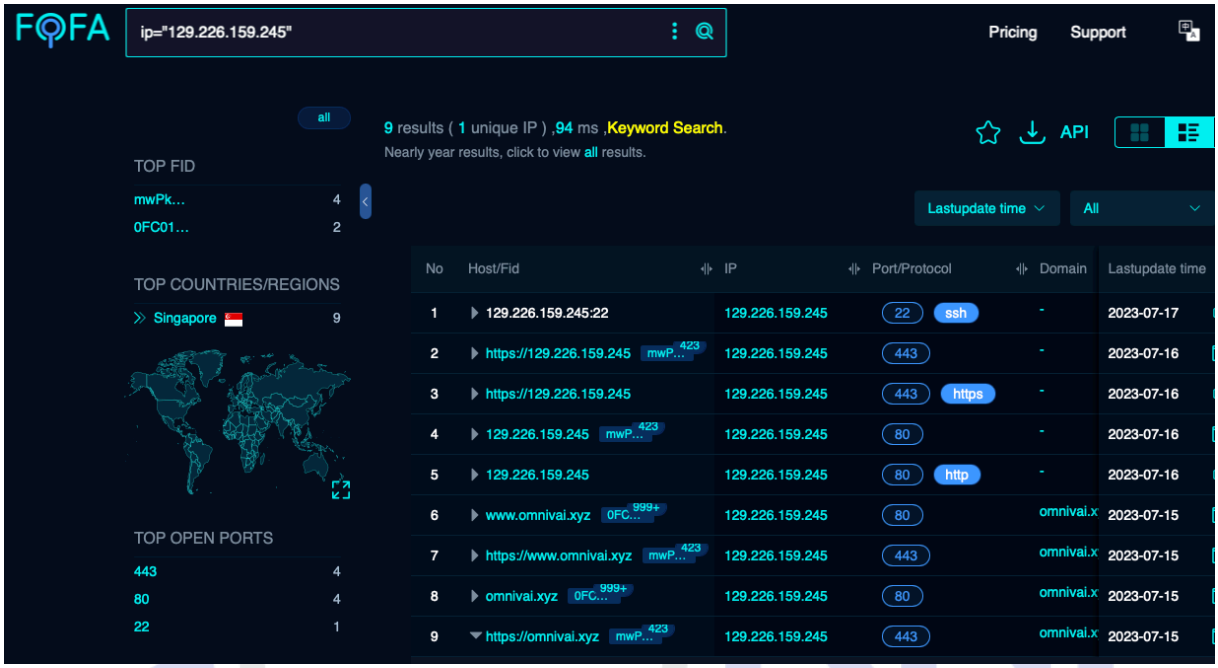
Passive DNS:

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

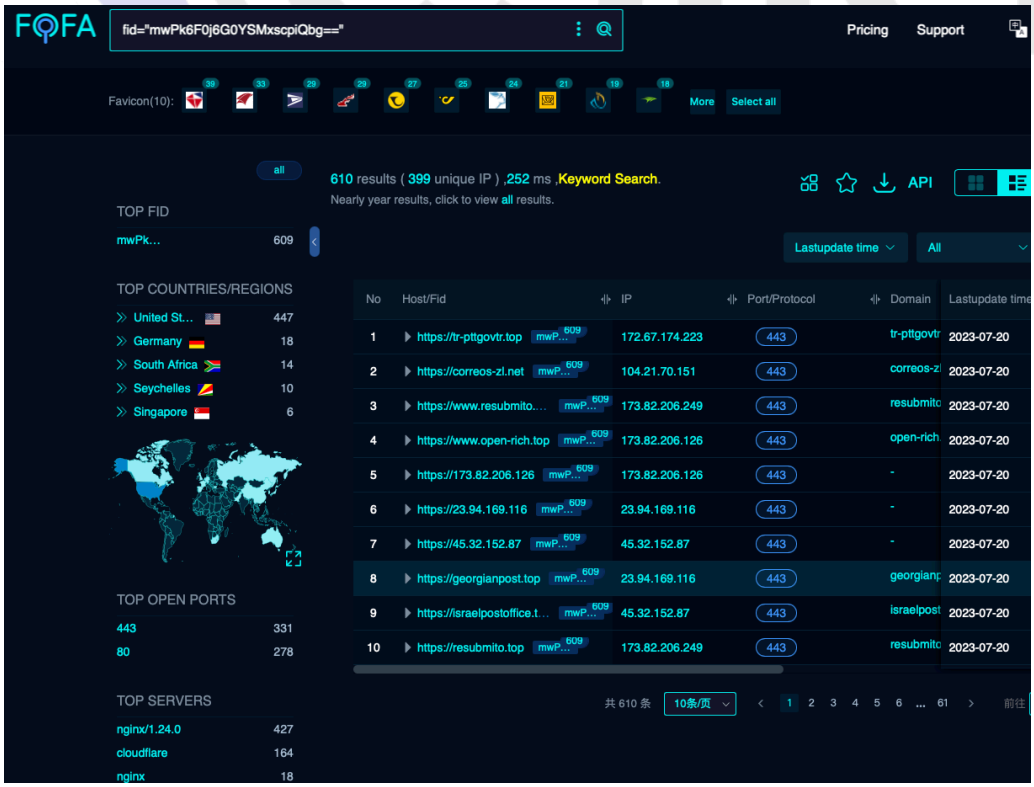


Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

FOFA.info:
Query: ip="129.226.159.245"



FOFA.info FID:
Query: fid="mwPk6F0j6G0YSMxscpiQbg=="



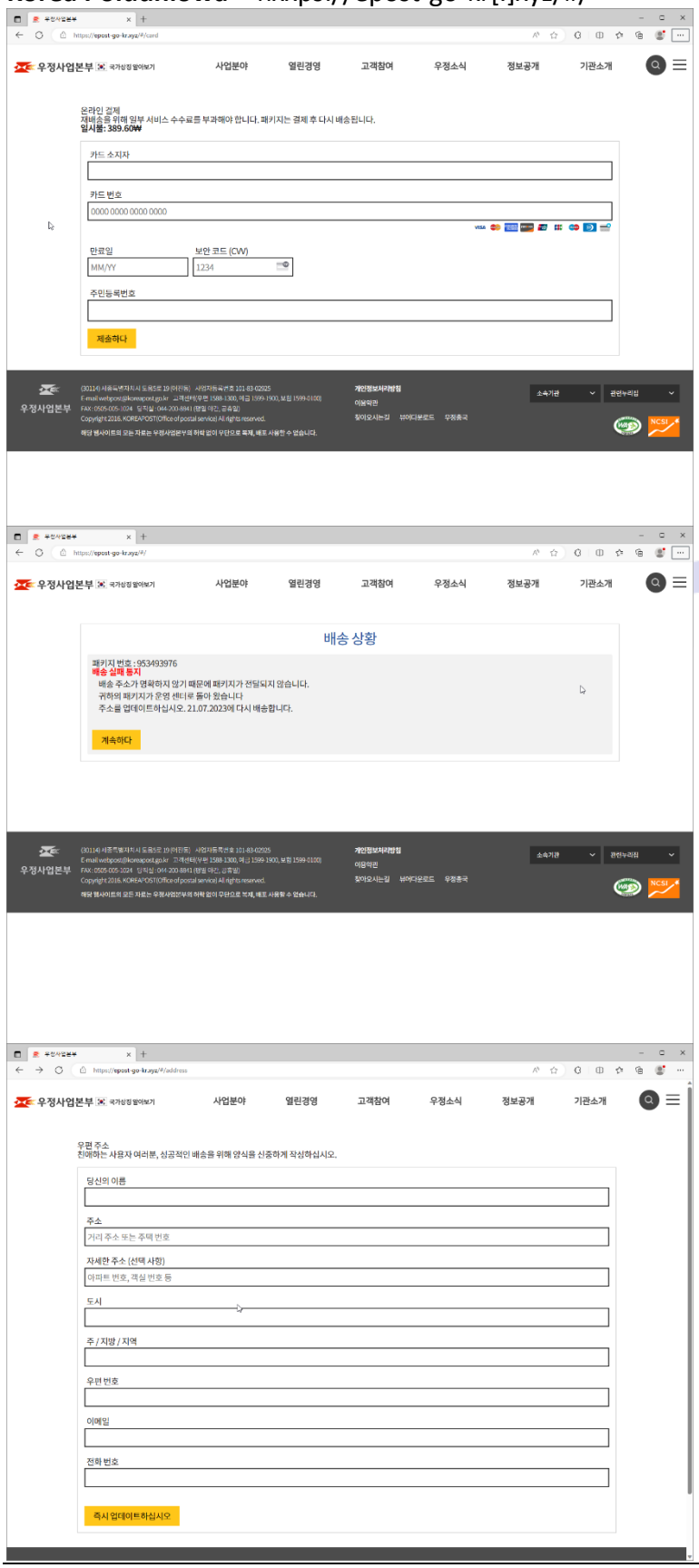
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

Favicon:

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

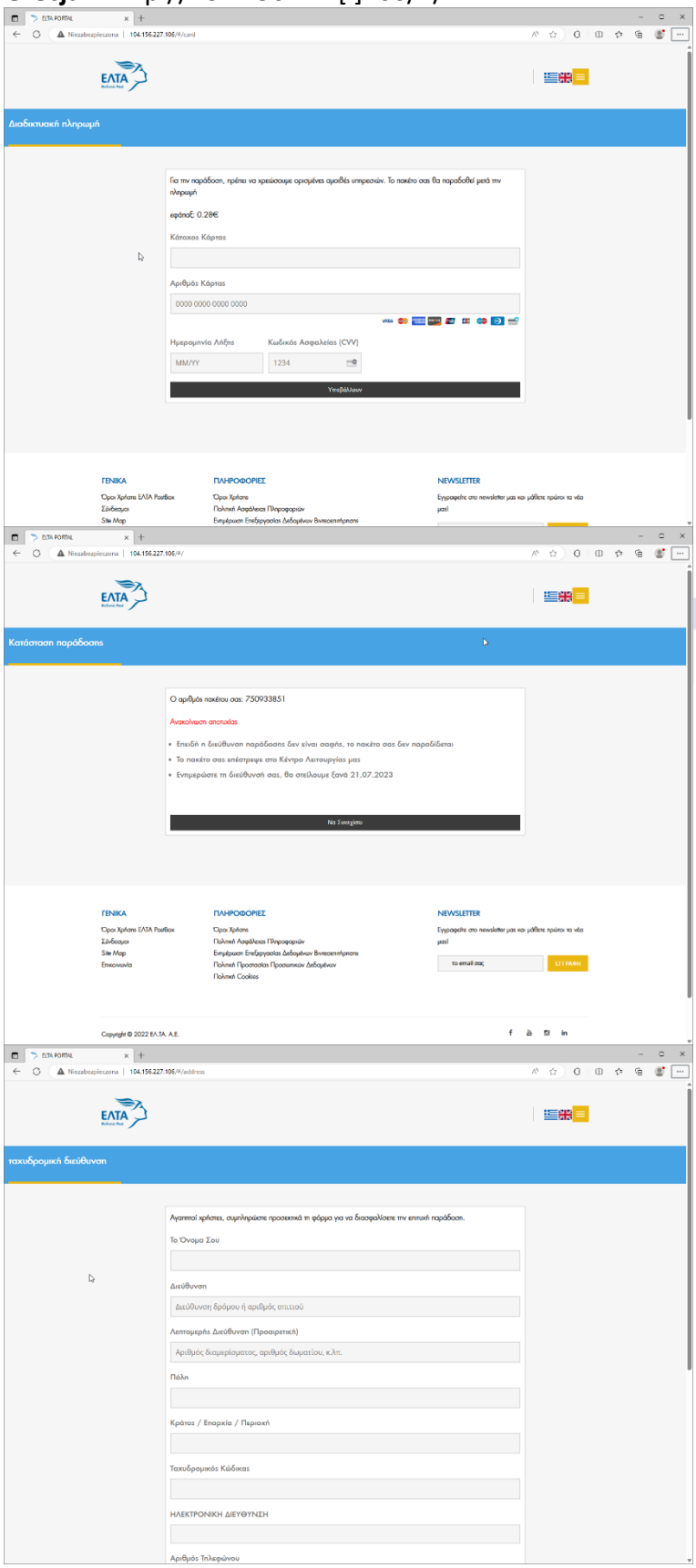
Zidentyfikowane oraz aktywne strony phishingowe na dzień 20.07.2023:

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



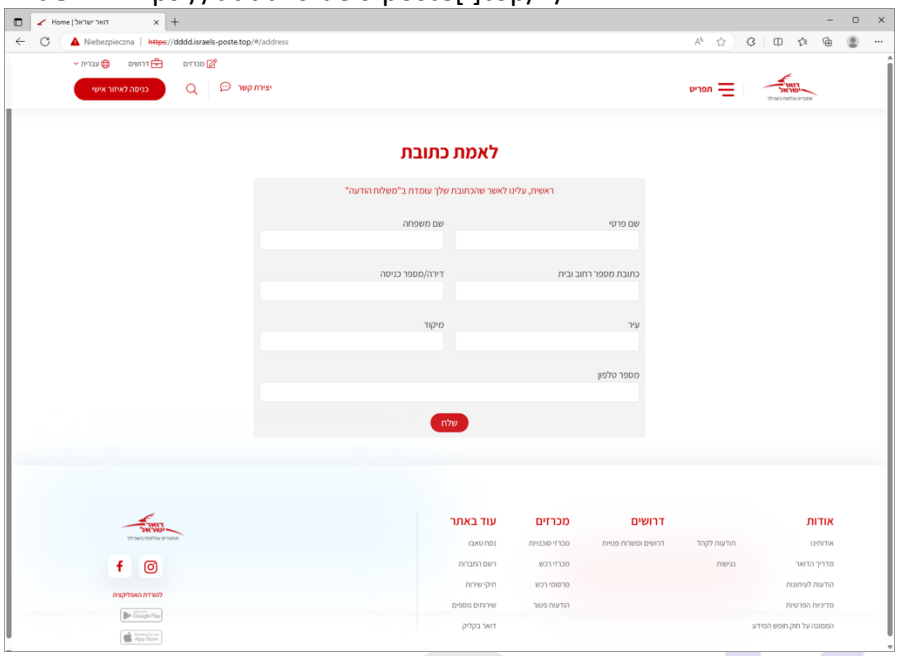
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

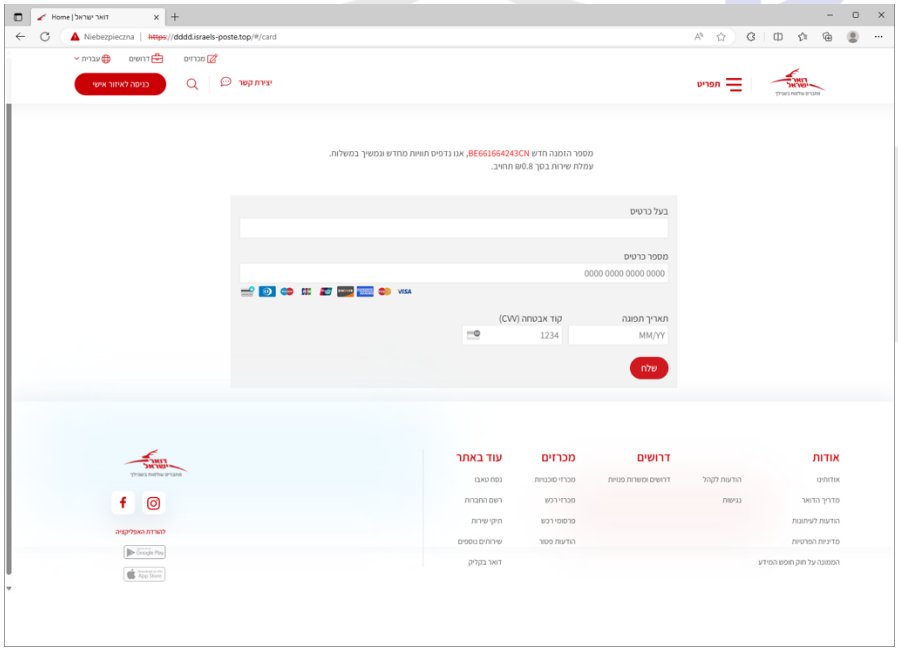
Grecja - hxxp://104.156.227[.]106/#/



Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

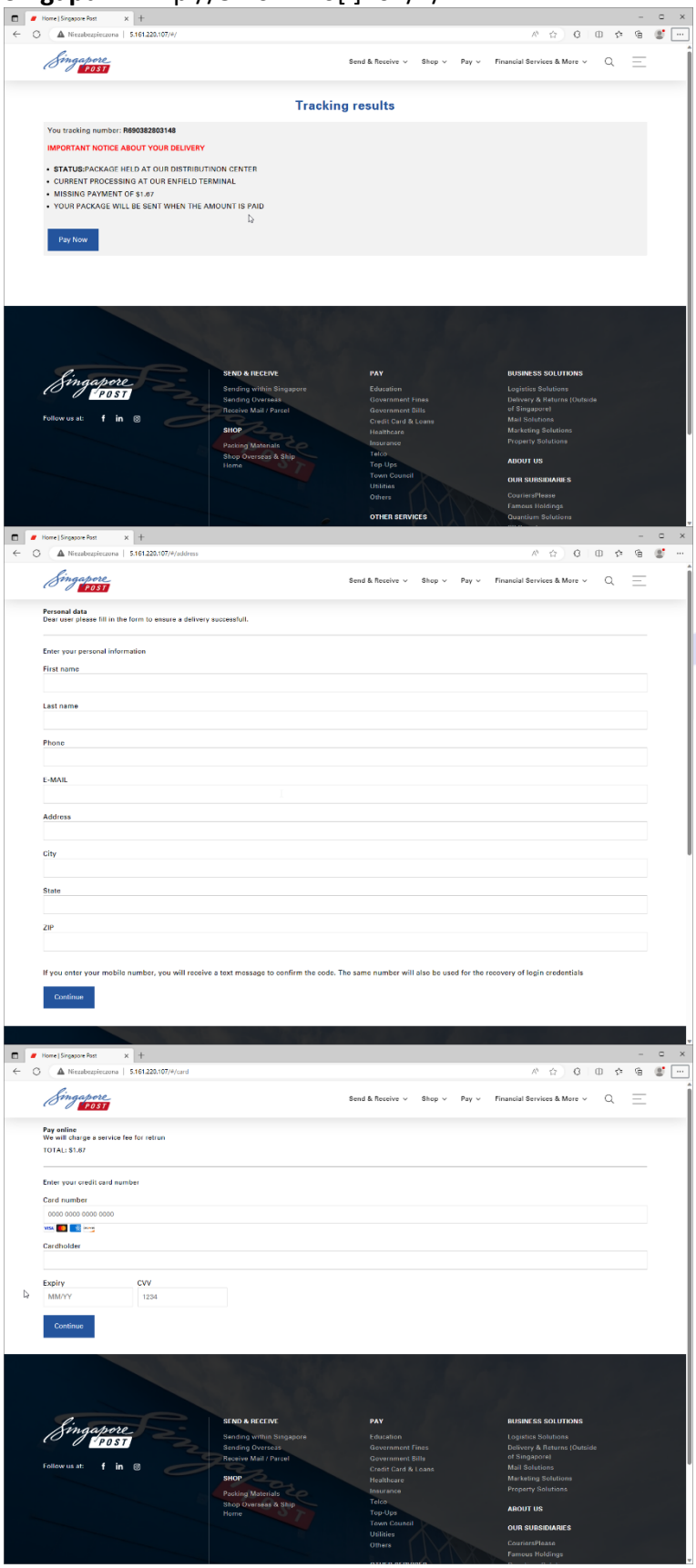
Izrael – hxxps://dddd.israels-poste[.]top/#/





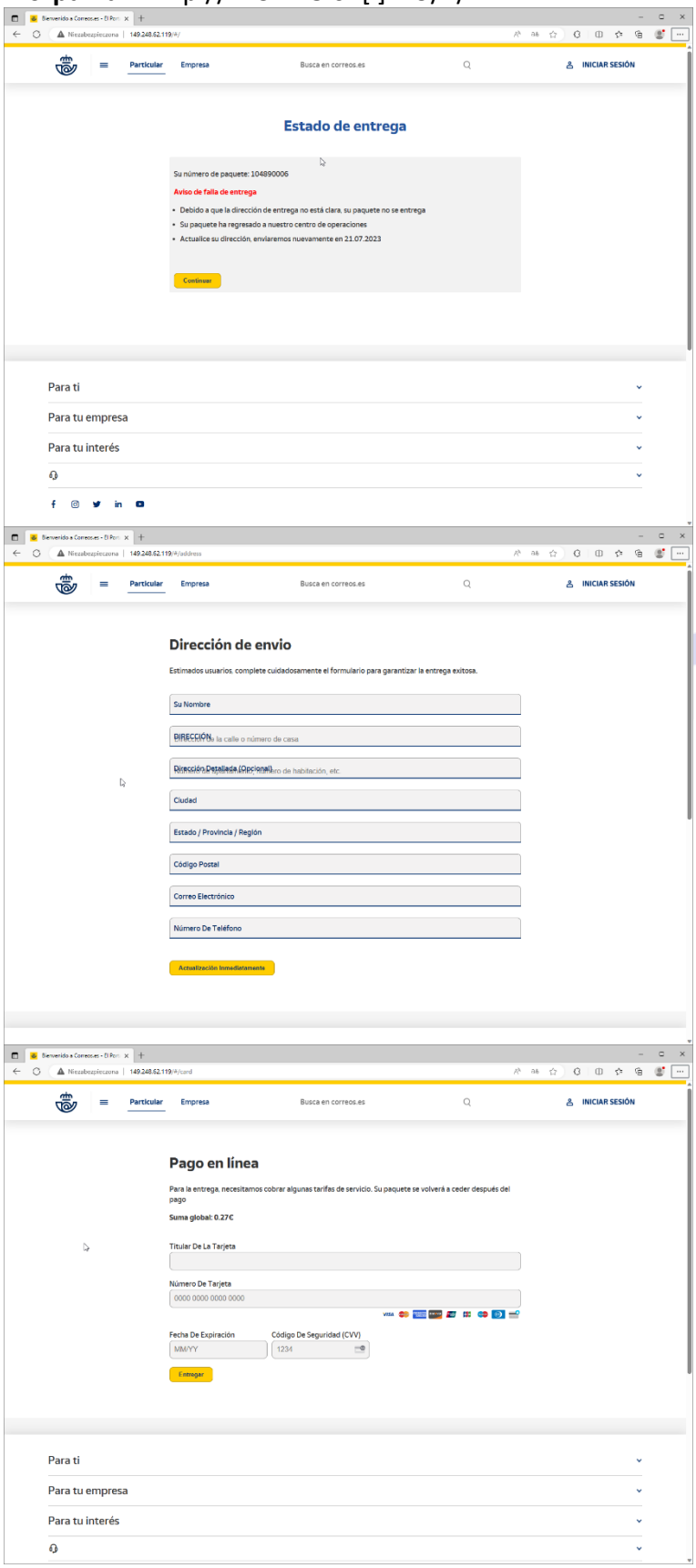
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



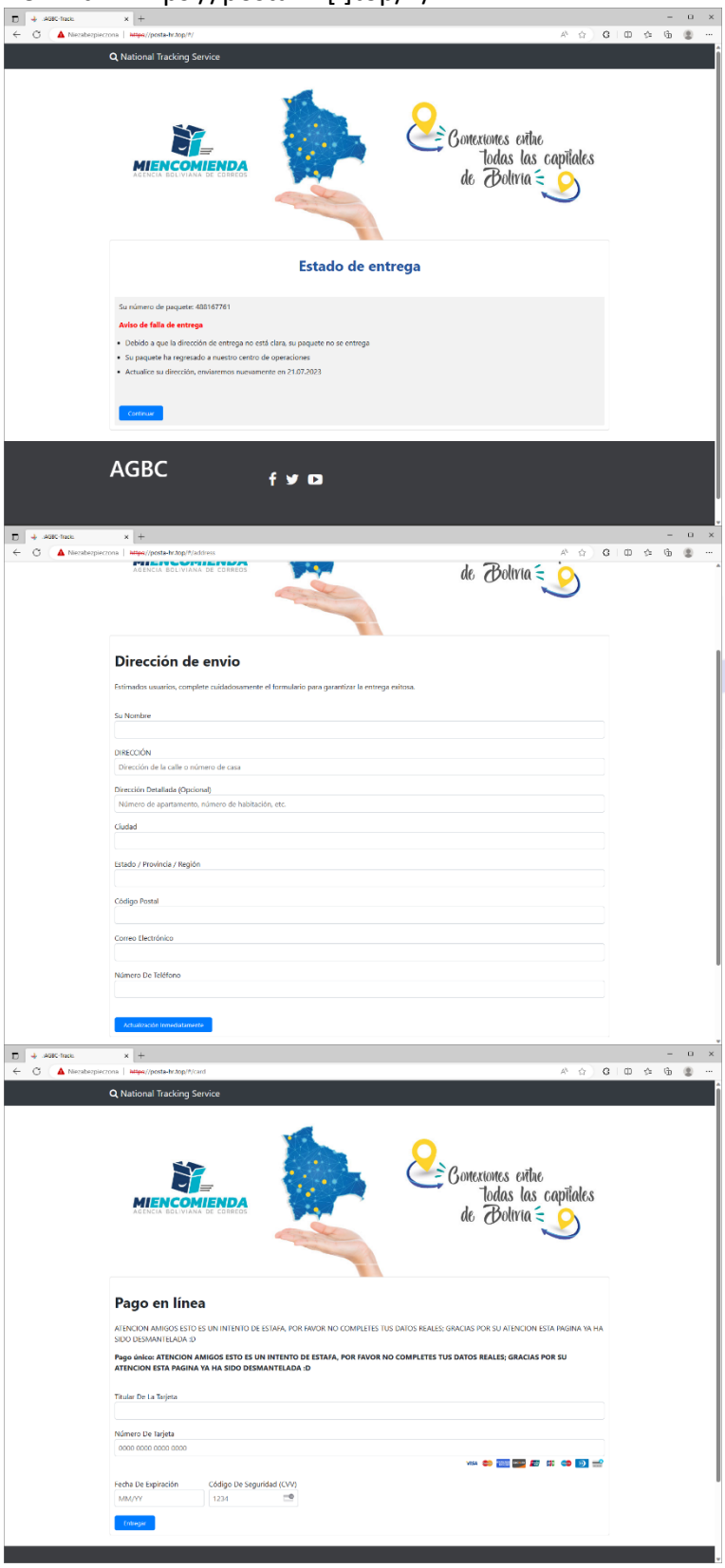
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



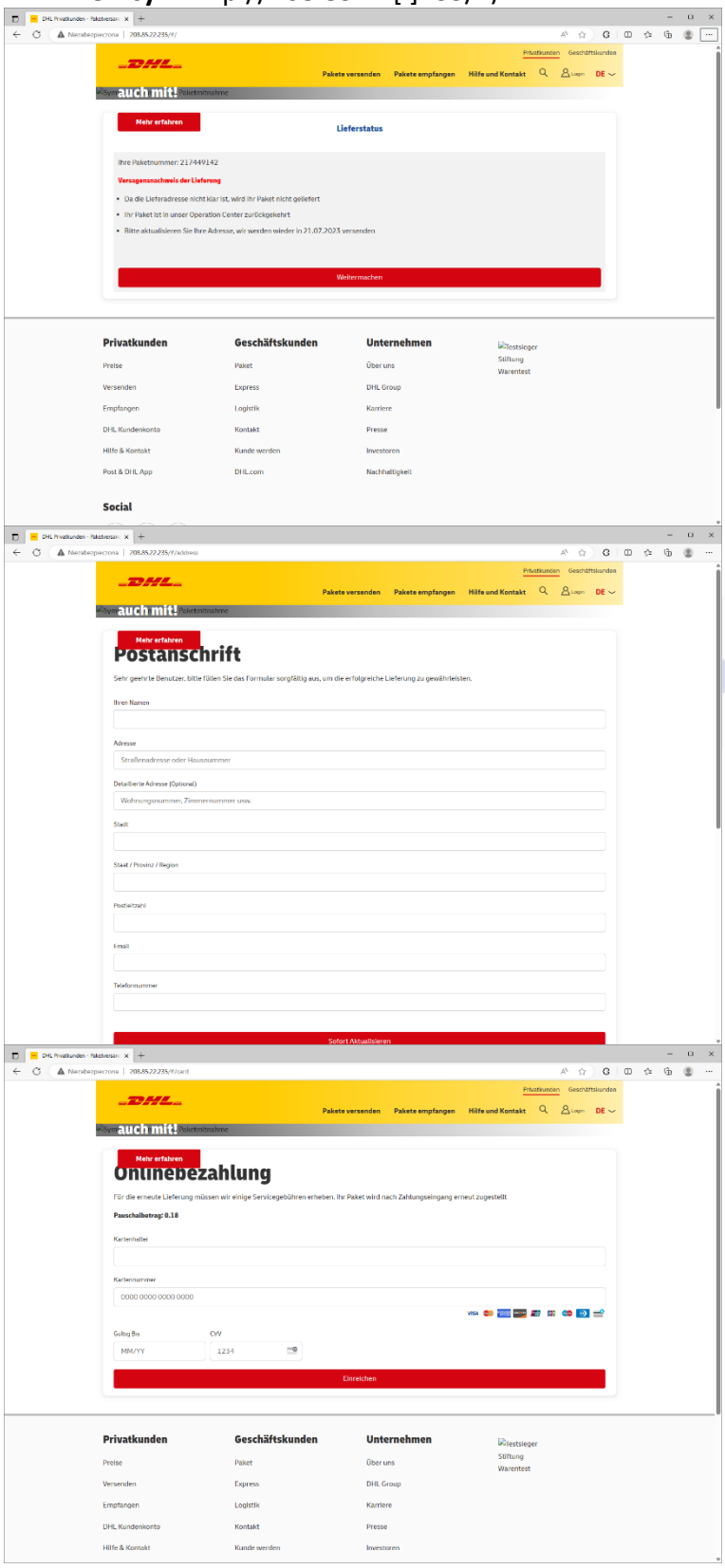
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



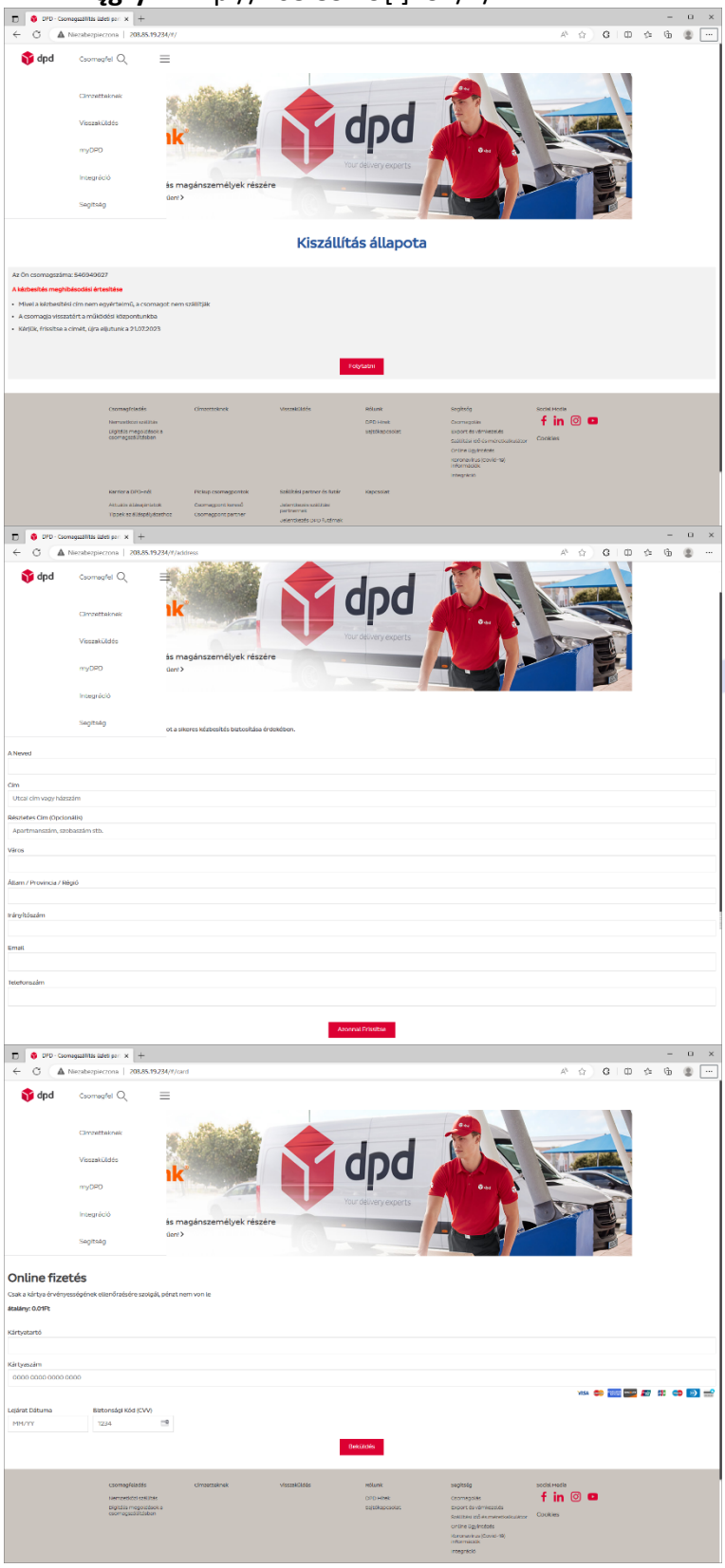
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



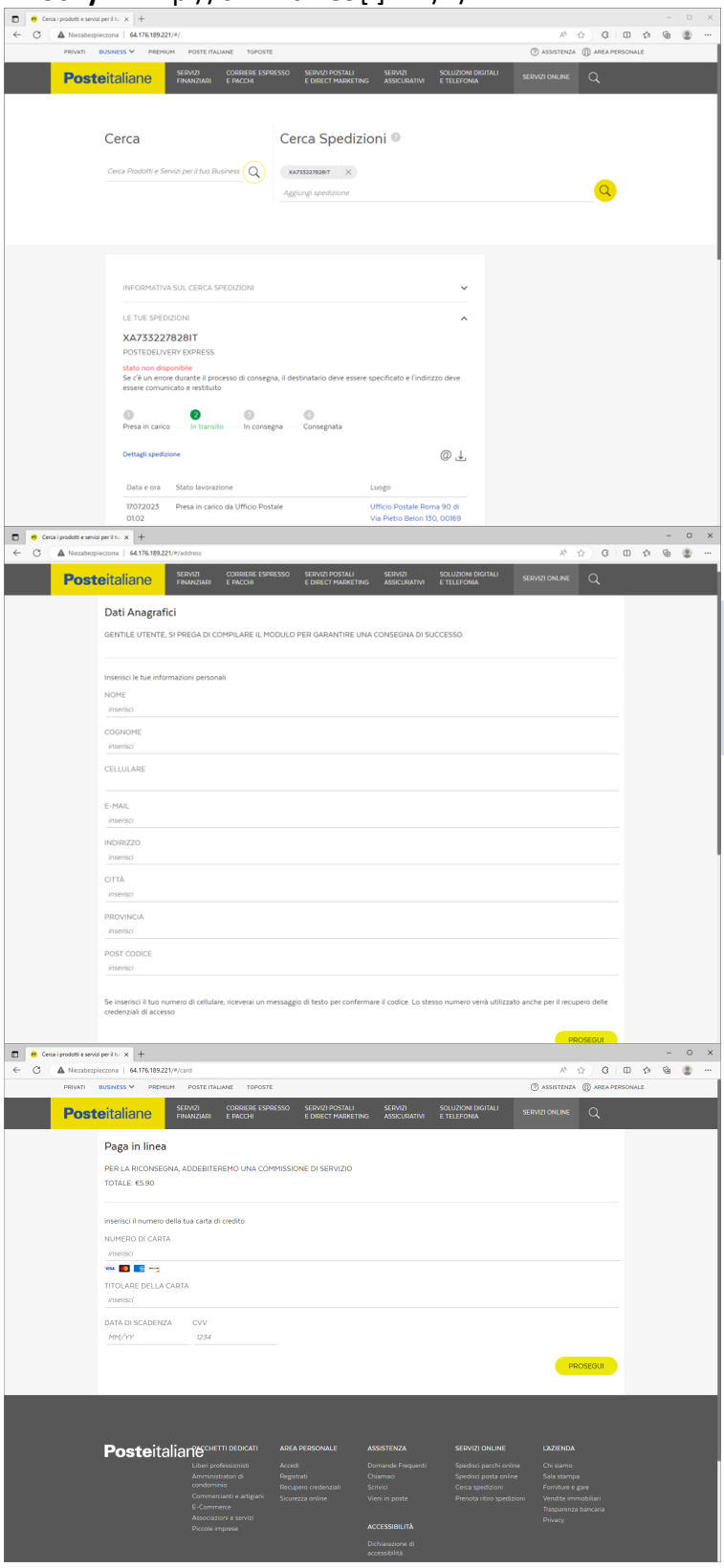
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

DPD Węgry - hxxp://208.85.19[.]234/#/



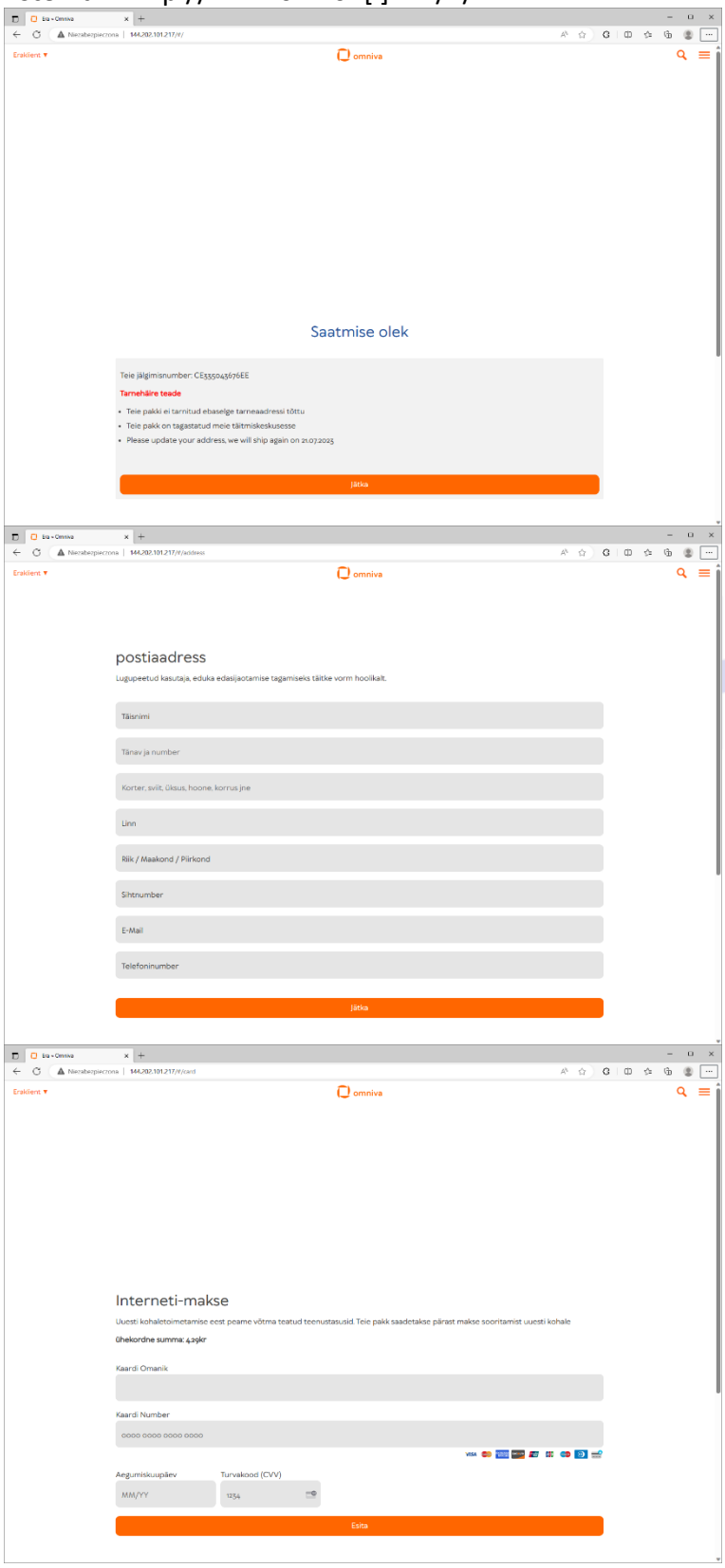
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

Włochy – hxxp://64.176.189[.]221/#/



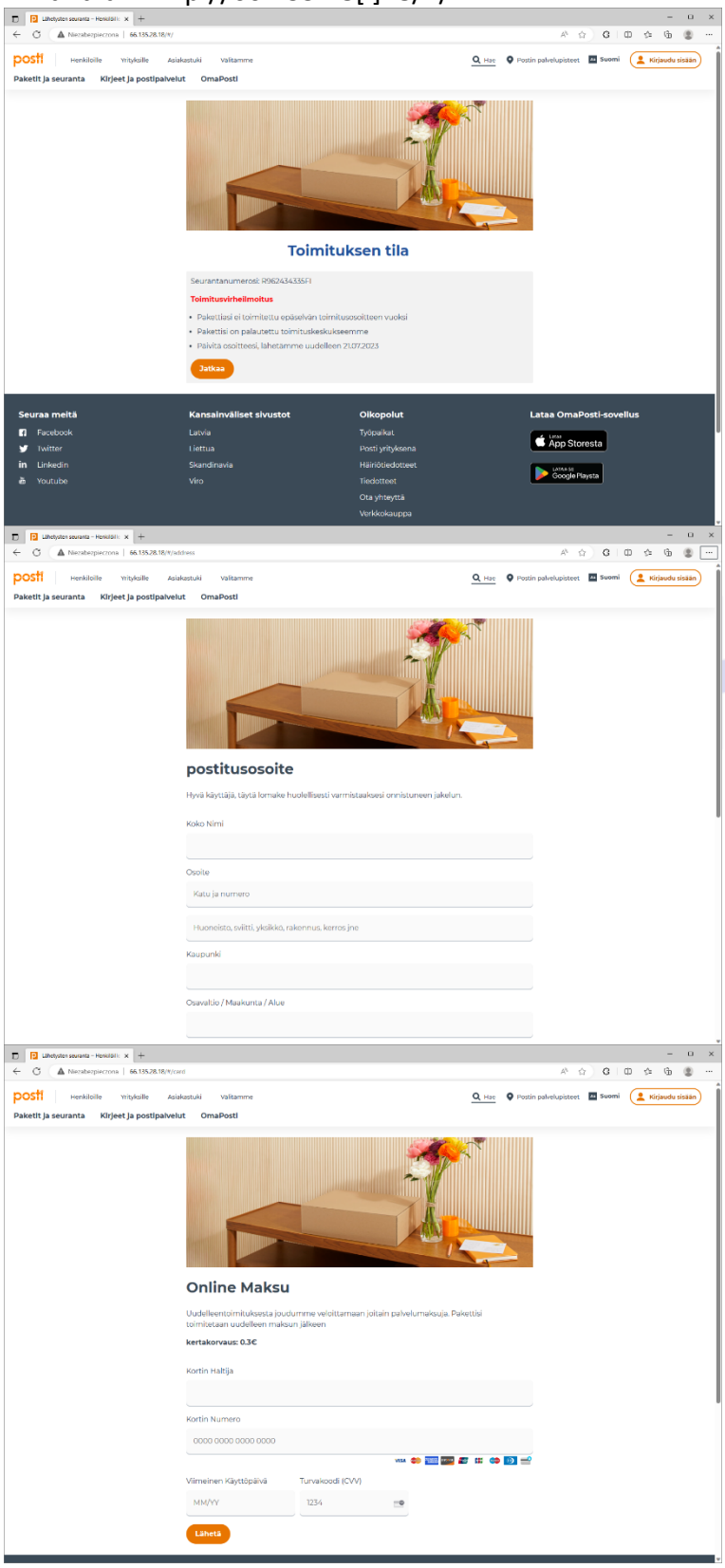
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



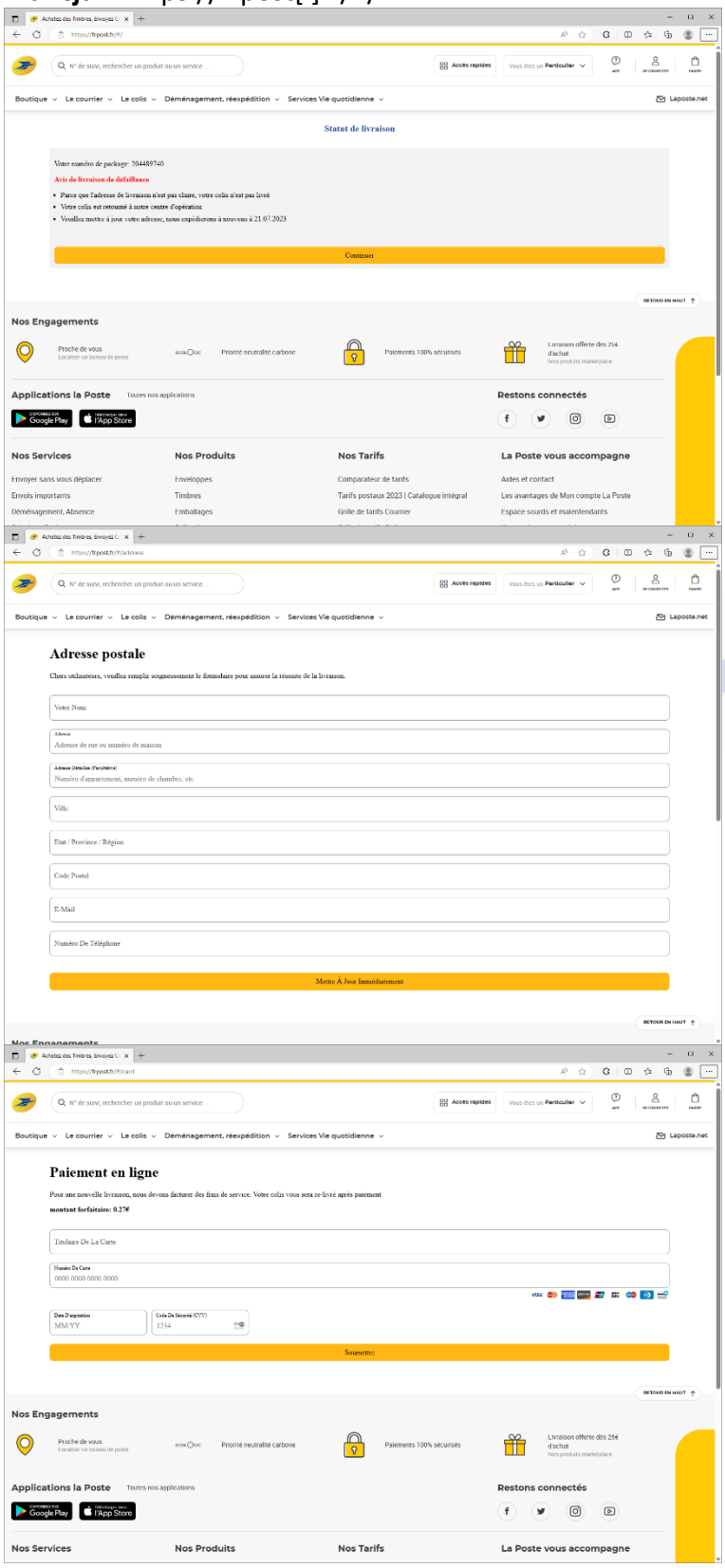
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



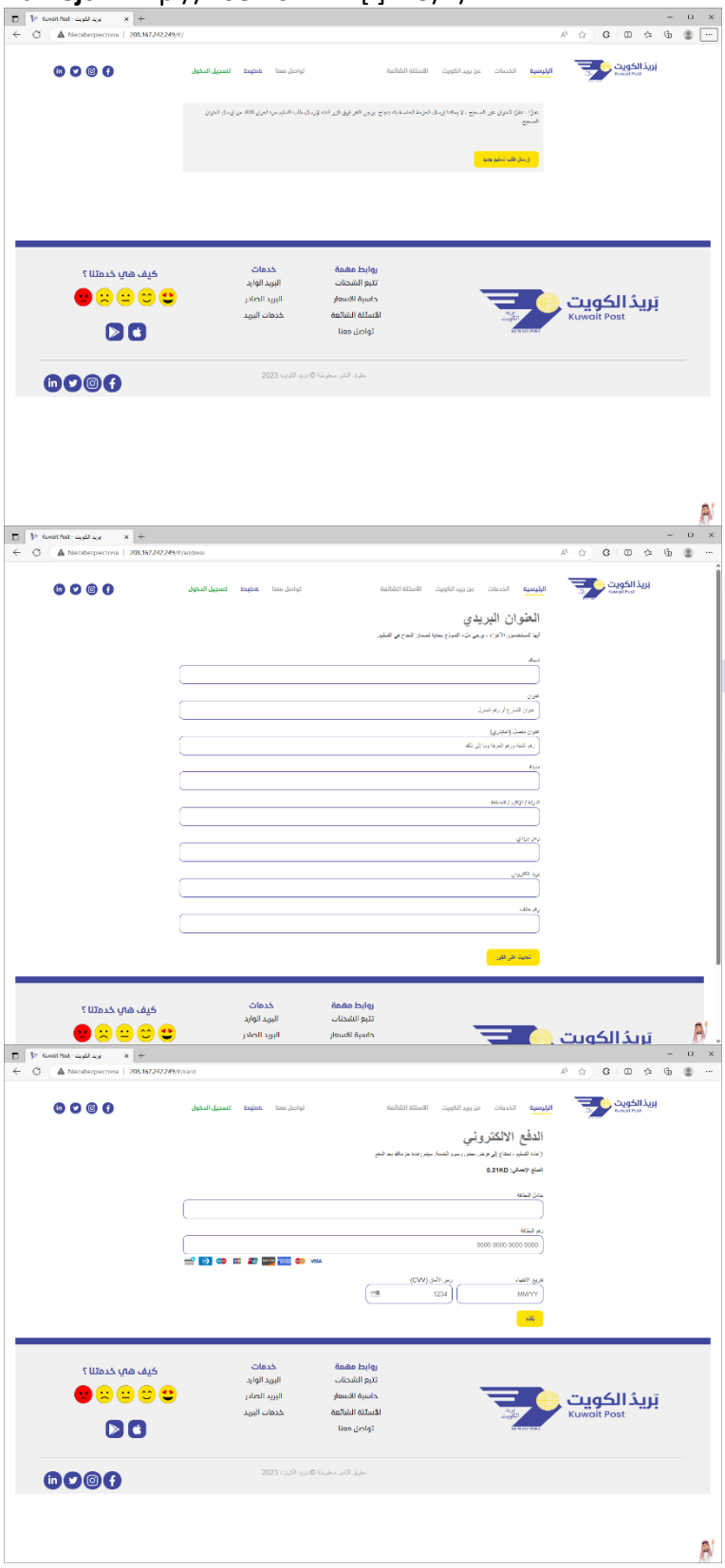
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



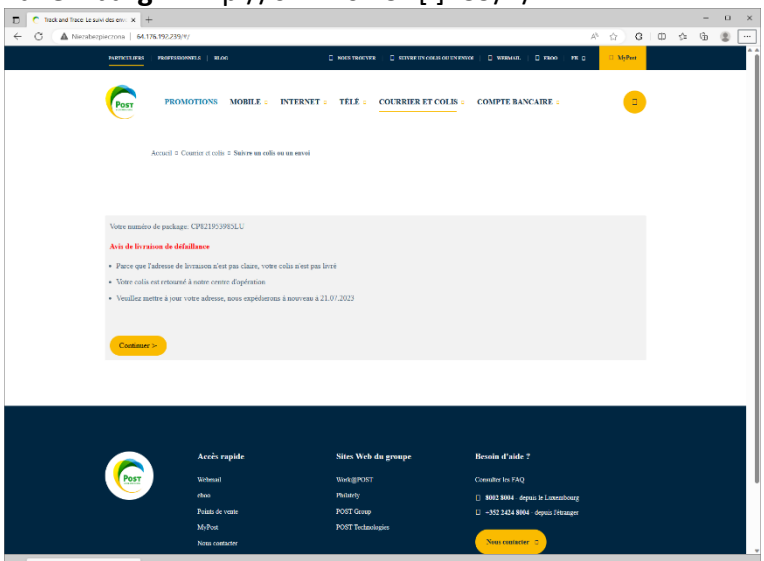
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

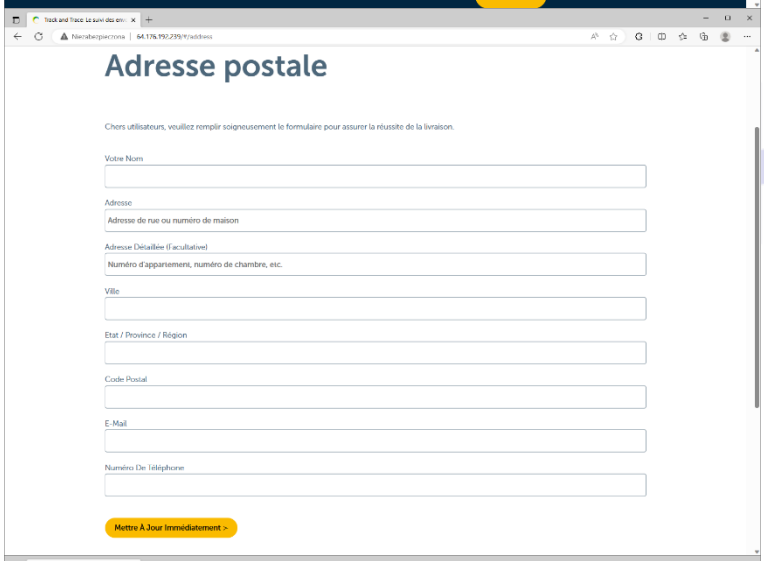
Kuwejt - hxxp://208.167.242[.]249/#/

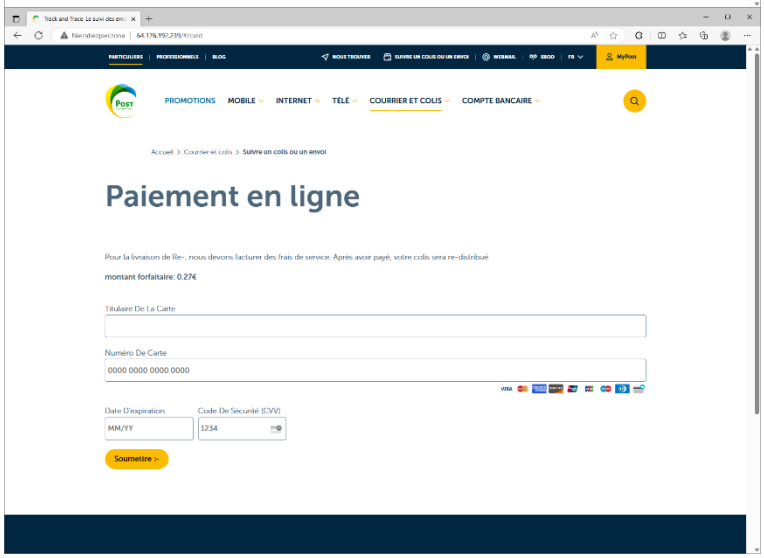


Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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

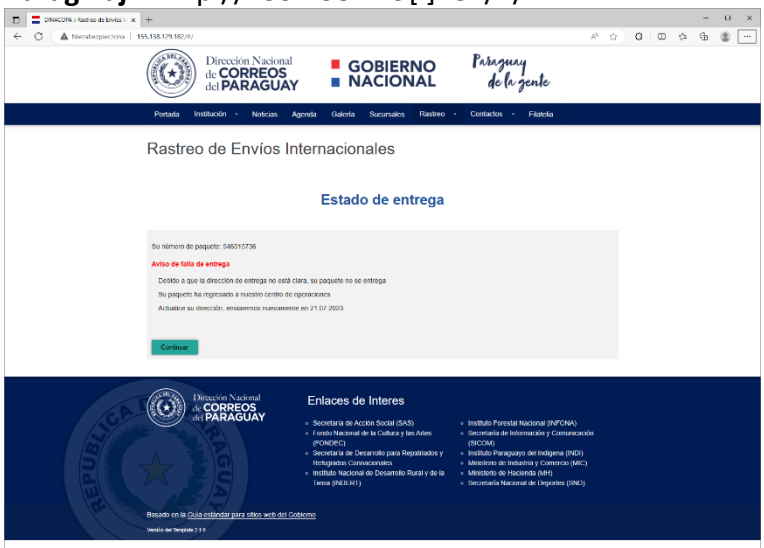


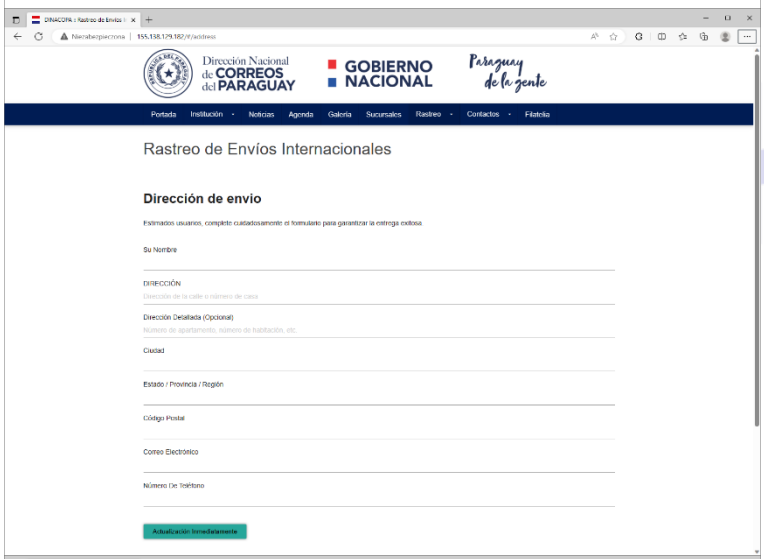


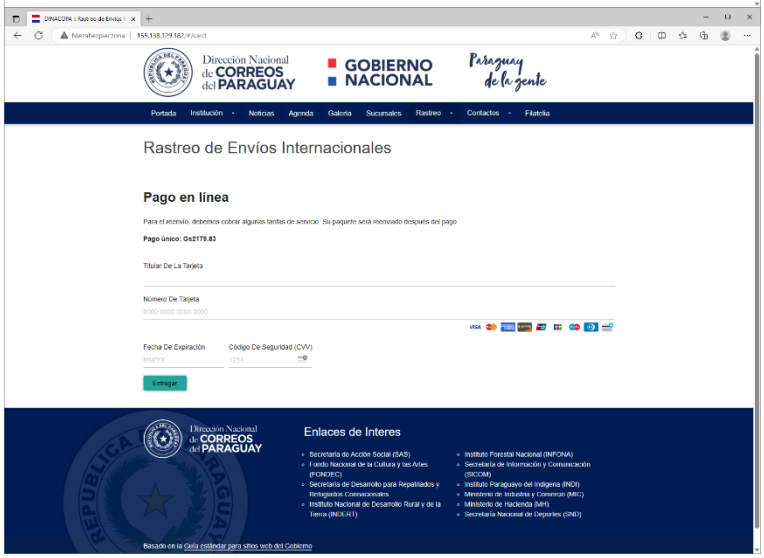


Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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

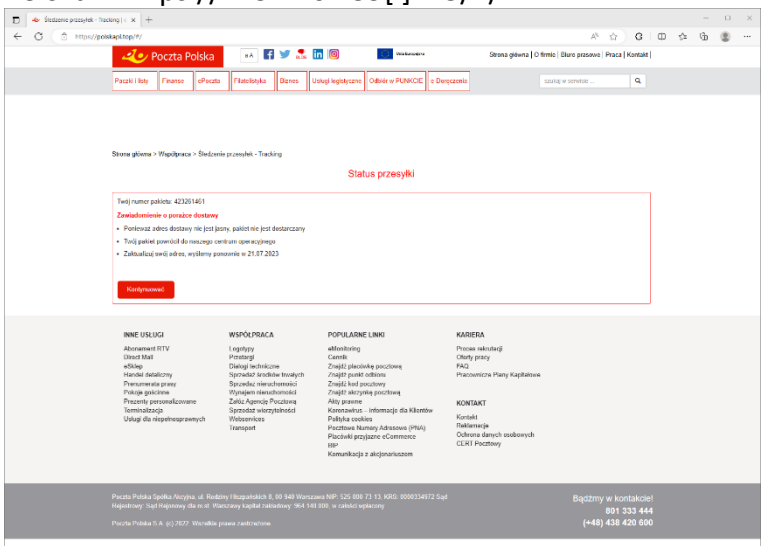


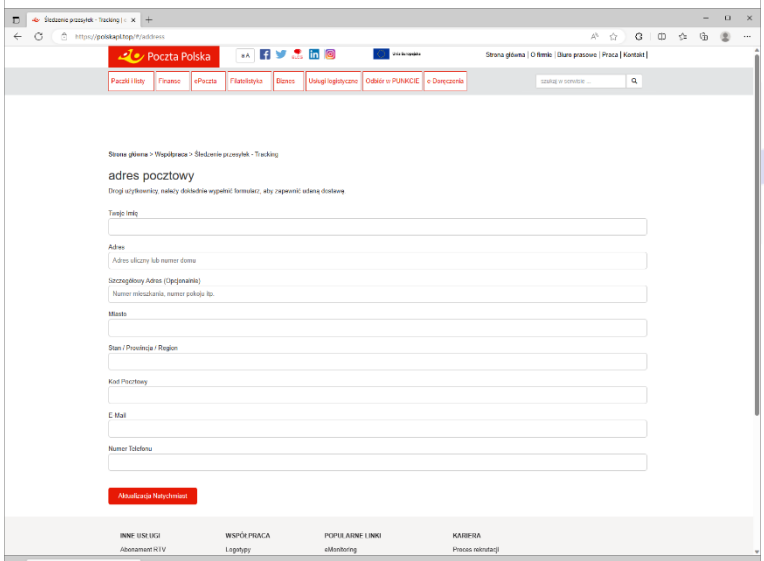


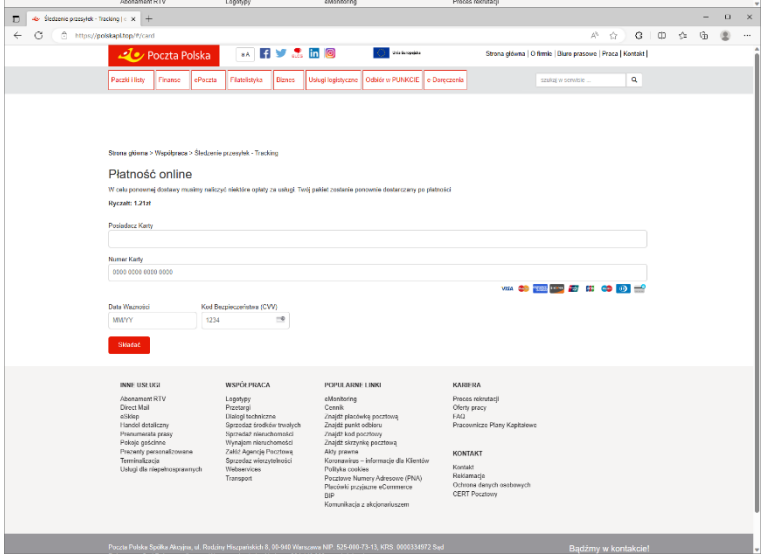


Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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

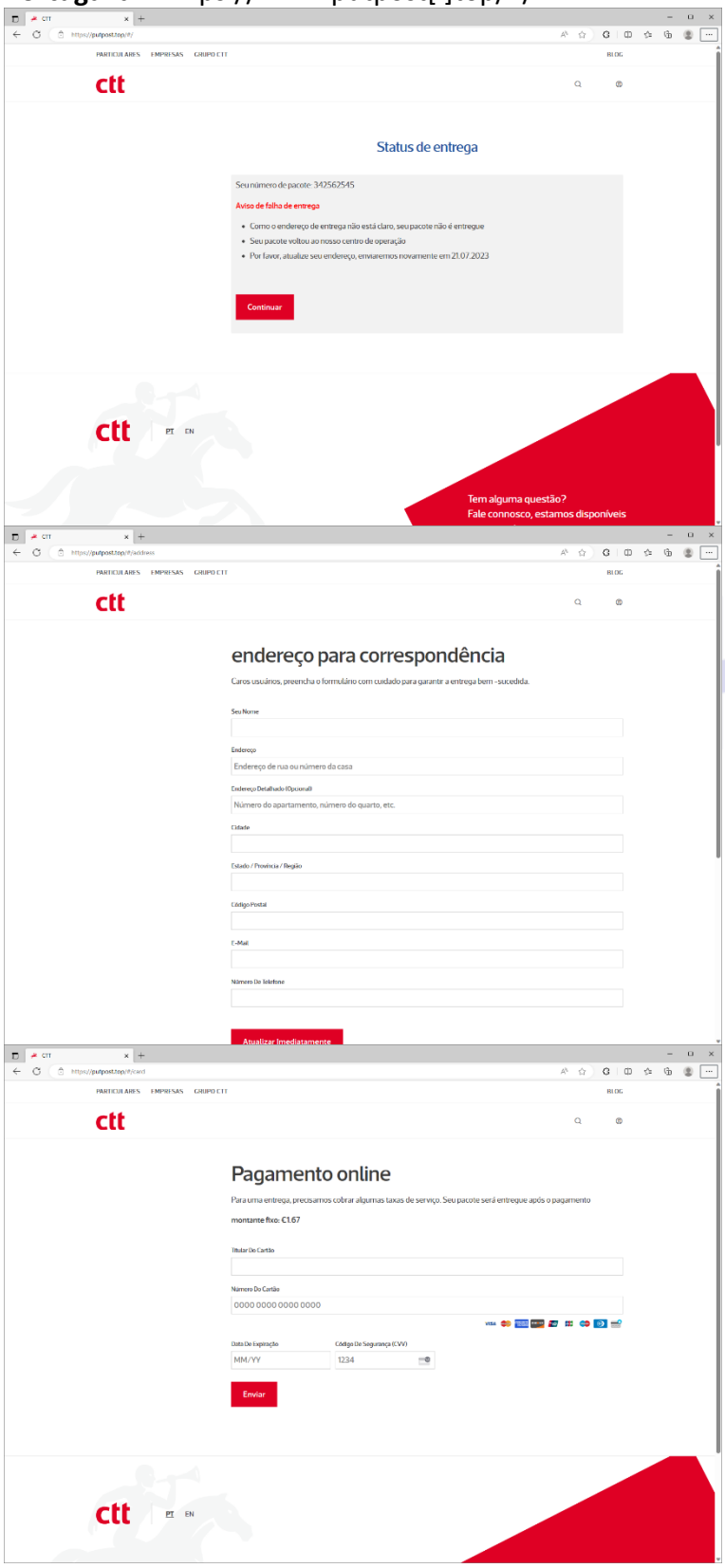






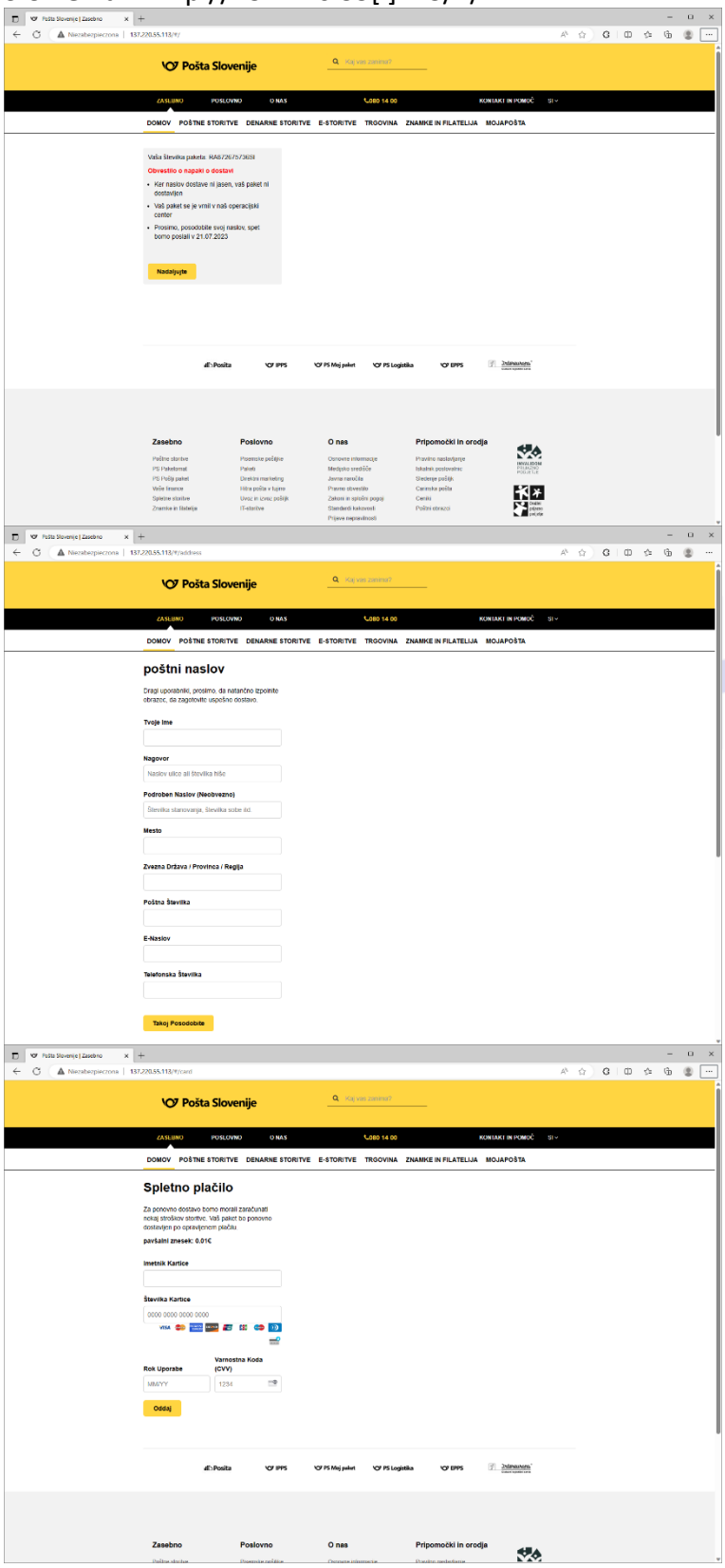
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



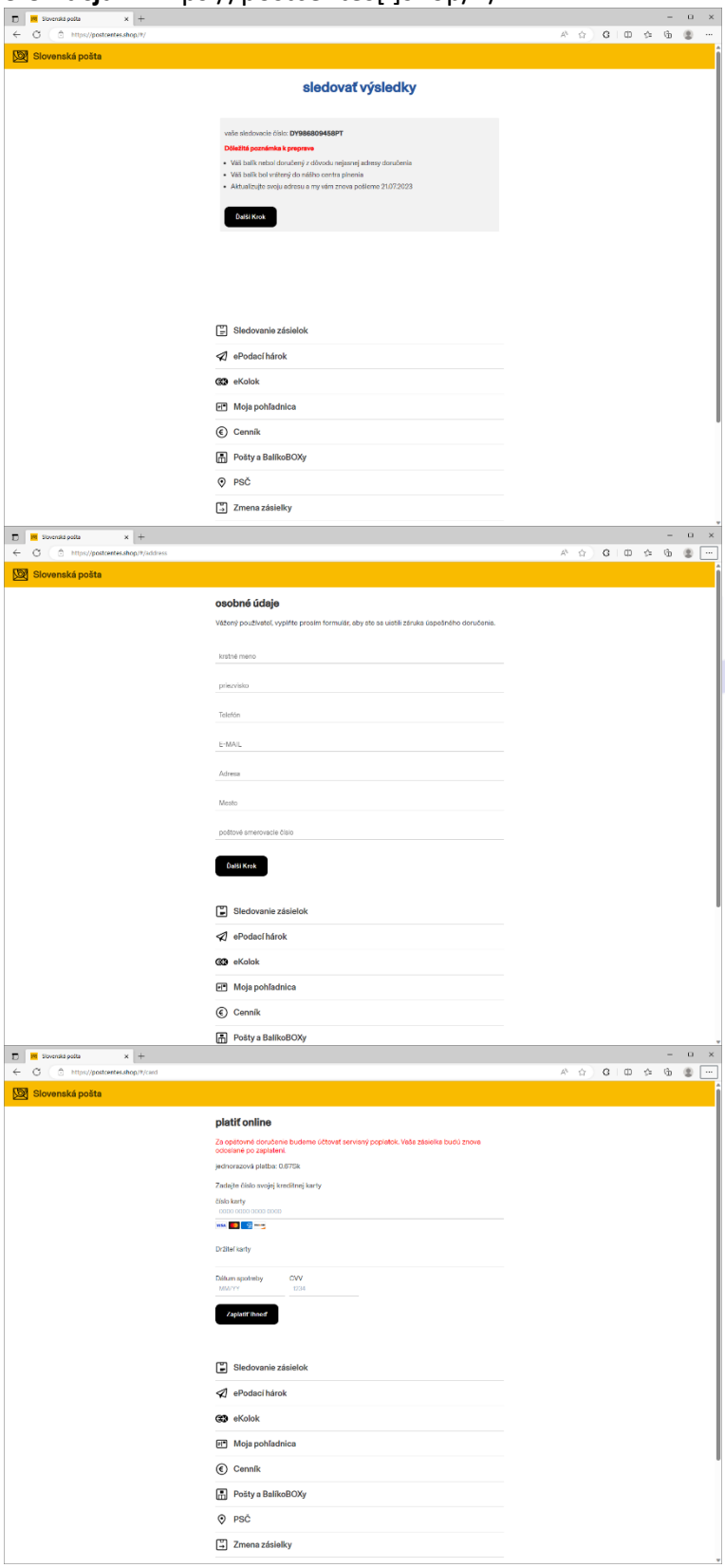
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

Słowenia - hxxp://137.220.55[.]113/#/



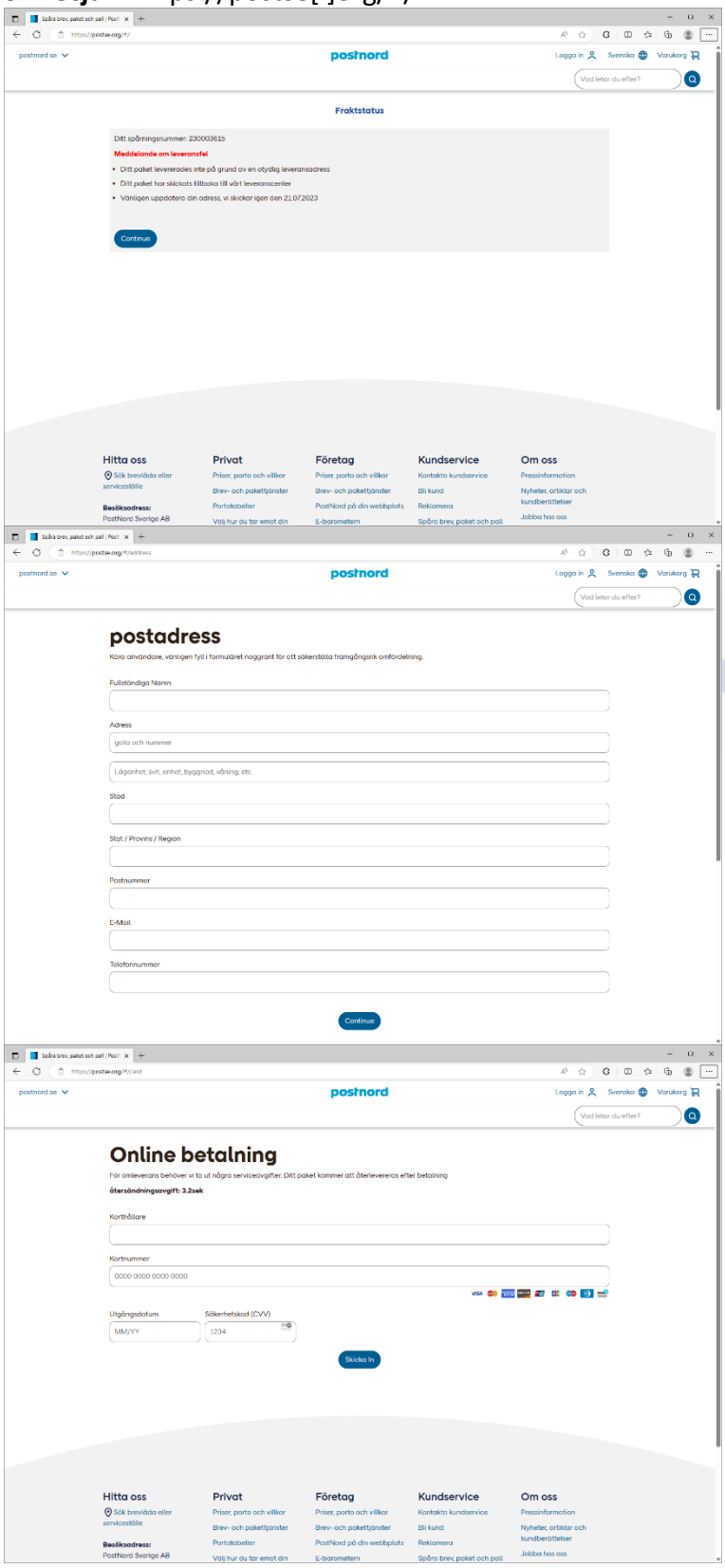
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



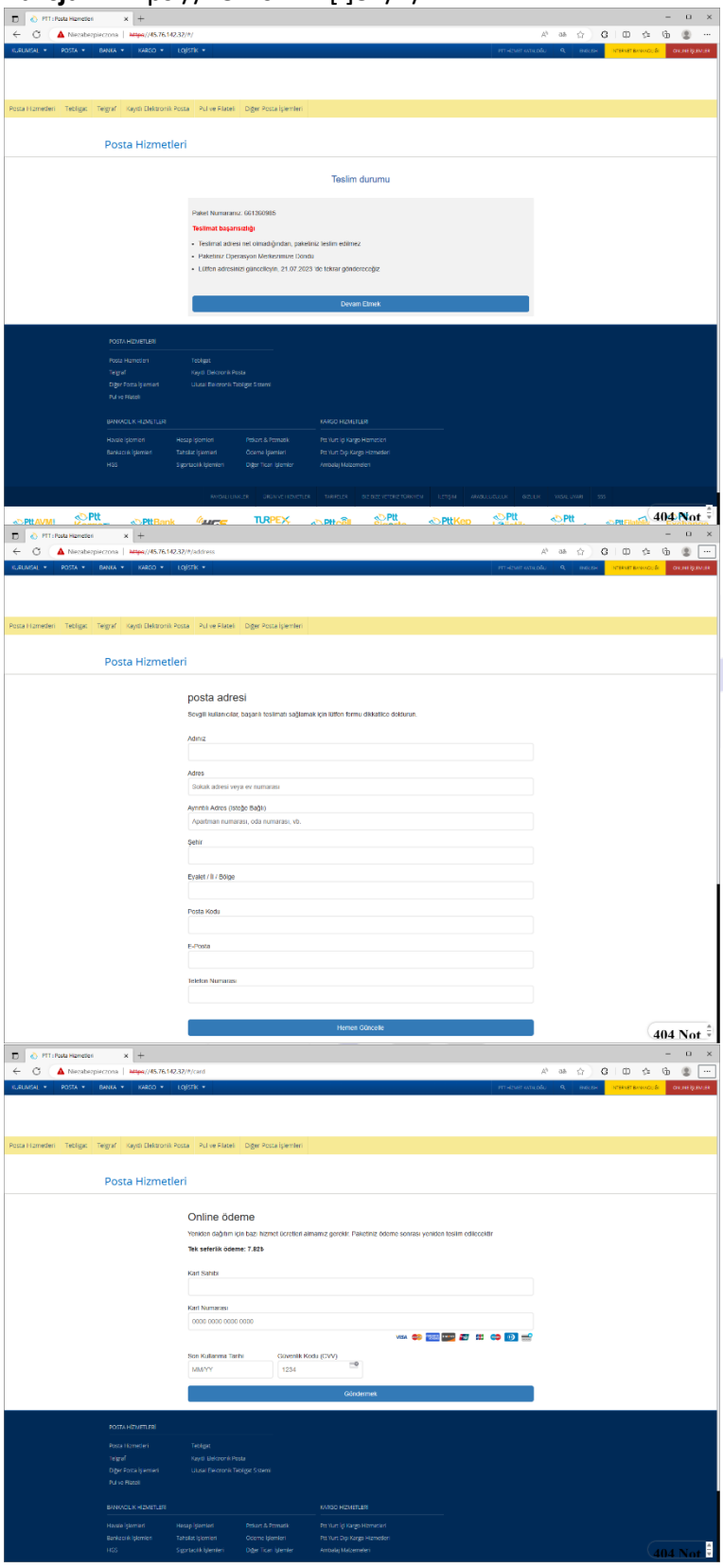
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



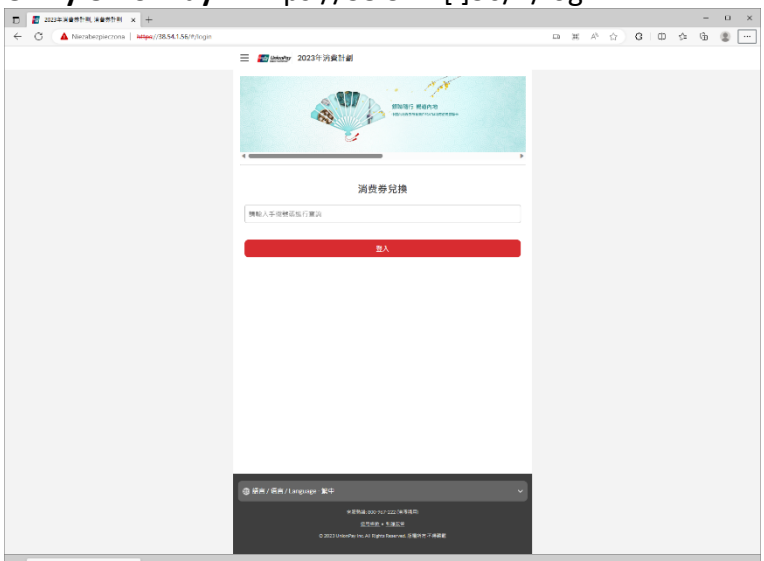
Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

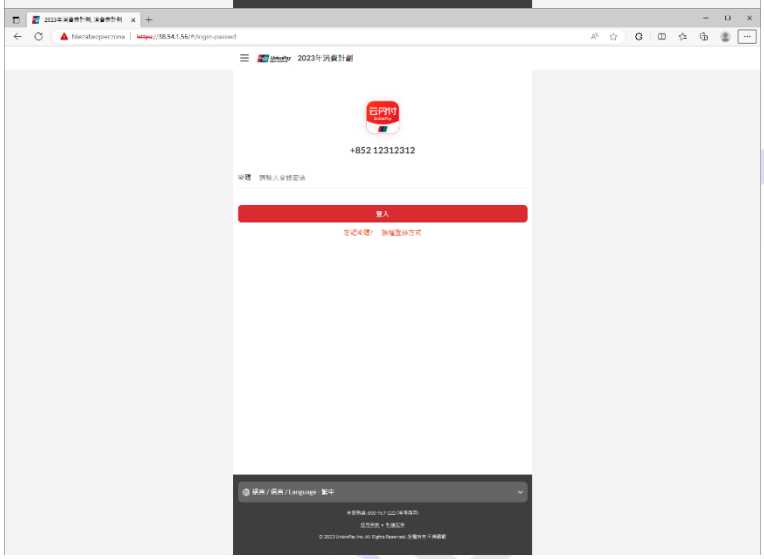
Turcja - hxxps://45.76.142[.]32/#/



Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

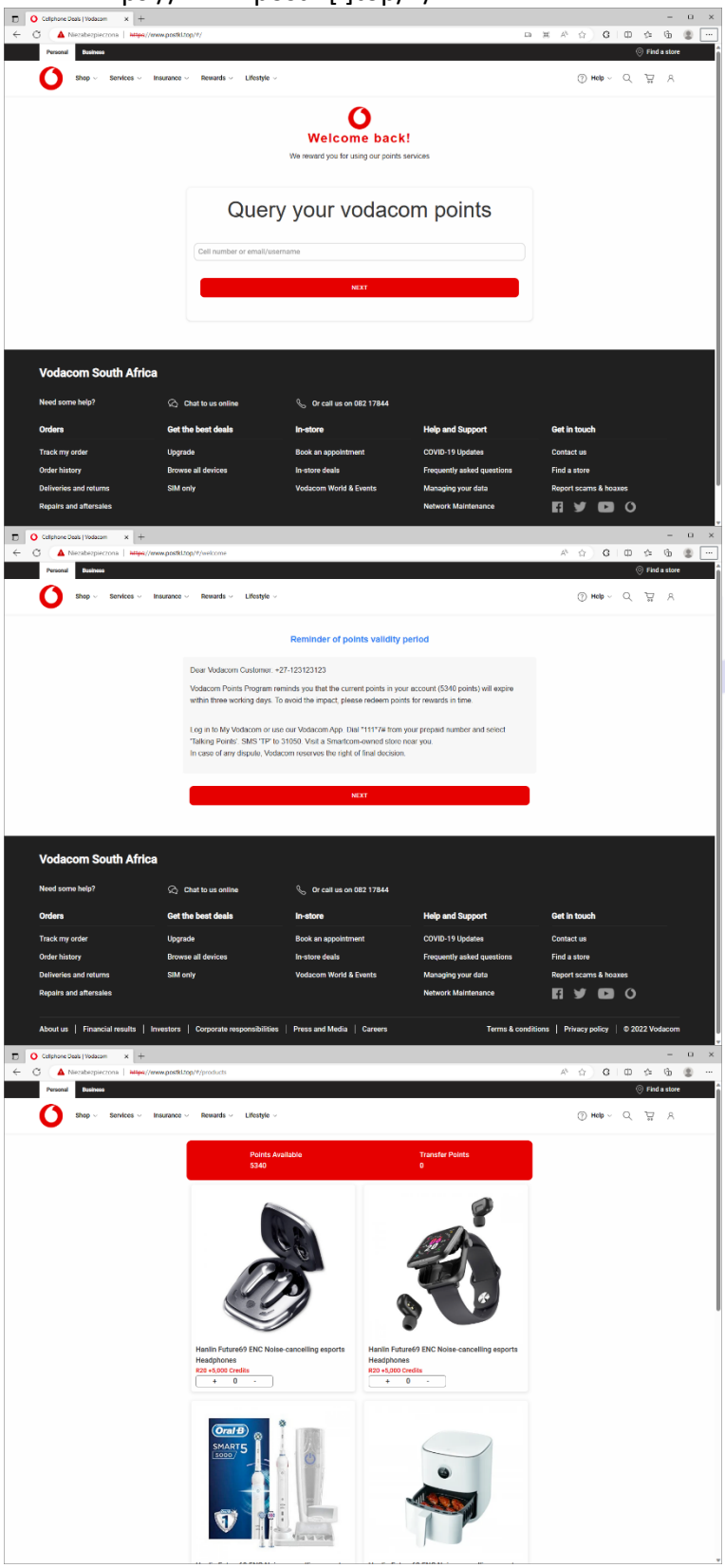
Chiny UnionPay - hxxps://38.54.1[.]56/#/login



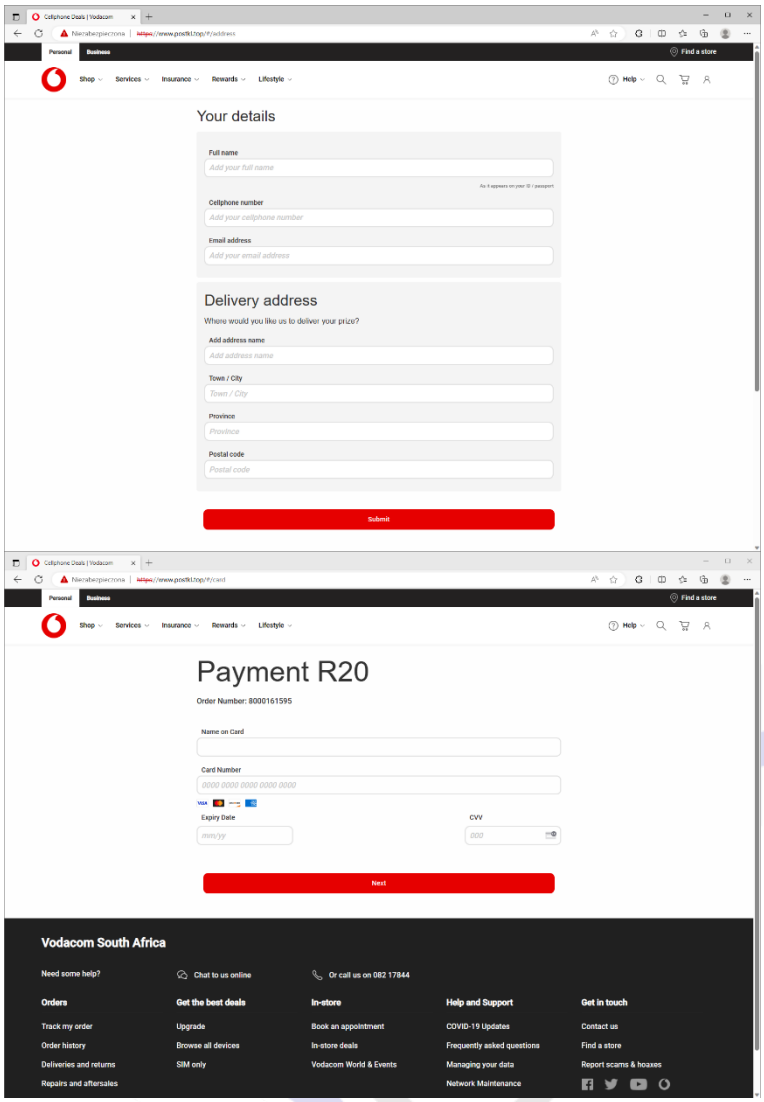


Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

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



Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF



Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

C2

Adresy IP:

'103.151.111.118',	'149.248.62.119',
'103.98.214.162',	'149.28.201.221',
'104.129.12.121',	'149.28.208.111',
'104.129.5.252',	'149.28.226.35',
'104.156.227.106',	'149.28.38.126',
'104.156.246.190',	'149.28.38.249',
'104.156.249.2',	'149.28.43.195',
'104.156.251.78',	'149.28.62.146',
'104.156.253.227',	'149.28.63.46',
'104.207.128.120',	'149.28.71.13',
'104.223.16.73',	'149.28.84.225',
'104.238.133.120',	'149.28.88.157',
'104.255.175.208',	'154.83.13.111',
'104.255.175.222',	'154.91.90.199',
'108.61.160.52',	'155.138.129.182',
'108.61.33.78',	'155.138.139.69',
'114.134.188.253',	'155.94.134.184',
'124.223.176.9',	'155.94.158.177',
'129.226.159.245',	'155.94.177.157',
'137.220.55.113',	'155.94.184.138',
'139.180.164.37',	'155.94.184.6',
'139.84.226.125',	'156.247.14.118',
'139.84.226.99',	'156.247.14.86',
'139.84.227.159',	'173.82.154.157',
'139.84.233.210',	'173.82.154.186',
'139.84.233.31',	'173.82.154.189',
'140.82.0.152',	'173.82.154.31',
'140.82.30.209',	'173.82.154.36',
'140.82.8.101',	'173.82.154.72',
'141.164.61.184',	'173.82.206.126',
'144.202.0.28',	'173.82.206.137',
'144.202.101.217',	'173.82.206.196',
'144.202.103.83',	'173.82.206.197',
'144.202.114.215',	'173.82.206.235',
'144.202.125.124',	'173.82.206.249',
'144.202.3.244',	'173.82.206.3',
'144.202.4.59',	'173.82.206.56',
'144.202.83.235',	'173.82.212.178',
'149.248.19.0',	'173.82.212.186',

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

'173.82.212.214',	'198.148.118.175',
'173.82.212.215',	'198.23.174.146',
'173.82.212.222',	'198.55.102.75',
'173.82.212.235',	'198.55.106.95',
'173.82.212.252',	'198.55.122.45',
'173.82.219.159',	'204.152.210.108',
'173.82.219.165',	'204.44.108.203',
'173.82.219.213',	'204.44.108.223',
'173.82.219.3',	'204.44.108.224',
'173.82.219.77',	'204.44.85.69',
'173.82.227.117',	'207.148.28.224',
'173.82.227.33',	'207.148.28.49',
'173.82.232.105',	'207.246.102.100',
'173.82.232.212',	'207.246.105.140',
'173.82.232.60',	'207.246.112.85',
'173.82.235.173',	'207.246.124.250',
'173.82.235.191',	'207.246.126.63',
'173.82.235.245',	'207.246.65.116',
'173.82.240.112',	'207.246.80.243',
'173.82.240.130',	'207.246.94.203',
'173.82.240.146',	'207.246.99.46',
'173.82.240.50',	'208.167.242.249',
'173.82.240.87',	'208.83.236.51',
'173.82.245.184',	'208.85.19.234',
'173.82.245.51',	'208.85.20.150',
'173.82.255.152',	'208.85.22.235',
'173.82.255.164',	'208.85.23.97',
'173.82.255.166',	'23.94.169.116',
'173.82.255.167',	'23.94.169.14',
'173.82.255.19',	'23.94.169.144',
'173.82.255.249',	'23.94.197.141',
'173.82.255.43',	'23.94.199.14',
'173.82.255.72',	'23.94.207.106',
'173.82.255.93',	'23.94.207.108',
'192.161.56.19',	'23.94.207.144',
'192.227.177.161',	'23.95.173.174',
'192.227.177.177',	'23.95.233.133',
'192.227.177.179',	'34.90.241.250',
'192.227.190.110',	'38.54.1.56',
'192.227.190.157',	'38.54.24.11',
'195.58.48.175',	'38.54.27.114',
'195.58.49.180',	'38.54.63.125',
'195.58.49.48',	'38.54.63.216',
'198.148.118.153',	'38.54.94.67',

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

'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'

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

Domeny:

'an-post.xyz',	'cri-poste-server.top',
'anpost-track.top',	'cri-poster-track.top',
'atpost.pro',	'cypruspost-post.services',
'ausposts.net',	'de-posts-dhl.top',
'autopase.top',	'dhighpu.xyz',
'autopass-no.cc',	'dpd-hu.top',
'autopass.bio',	'e1t5bpf2.com',
'autopassno-top.top',	'eeporstee.com',
'autopassno.top',	'eeposte.net',
'avantrawr.shop',	'elta-help.top',
'bahrainpost.top',	'elta-new.top',
'bpost-be.top',	'elta-news.top',
'bpost.vip',	'elta-post.top',
'ceskaposta.top',	'eltagr.monster',
'chl-correos.top',	'eltagr.one',
'chl-pose-server.top',	'eltagr.top',
'chl-poster-track.top',	'enposta.top',
'chl-postese-track.top',	'epost-go-kr.xyz',
'chl-postets-track.top',	'etc-jp-nexco-etc.top',
'chl-postse-track.top',	'foodnew.top',
'coles--au.shop',	'foodpandatw.top',
'coles-au.co',	'frpost.fr',
'coleș.com',	'georgianpost.top',
'correo.monster',	'govuk.top',
'correos-cl.cc',	'grupoice.vip',
'correos-cl.services',	'hellotoby.top',
'correos-cr.top',	'hk-shell.top',
'correos-es.mom',	'hrpost.co',
'correos-help.xyz',	'ias516fb.com',
'correos-poster.xyz',	'idme.red',
'correos-zl.net',	'instanthq.com',
'correos.boats',	'israeipost.top',
'correos.pics',	'israel-posts.top',
'correos.wang',	'israele-posts.top',
'correosbolivia.top',	'israelp-post.top',
'correosccc.top',	'israelpostoffice.top',
'correoscl.buzz',	'israels-poste.top',
'correosclo.top',	'jordanpost.top',
'correosgob.buzz',	'kaz-kazpster.top',
'correosgocr.co',	'kddi-au.top',
'correoso.top',	'krtopaes.top',
'correoss.online',	'krtopasoet.top',

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

'krtopeote-track.top',	'postask.buzz',
'krtopessoe-track.top',	'postasw.xyz',
'kuwaitpost.top',	'postcentes.cyou',
'luhg8p7a.com',	'postcentes.icu',
'moc-gov.world',	'postcentes.shop',
'nfipz.top',	'postcentes.xyz',
'norddk.com',	'postcentres.cloud',
'norwaypass.co',	'postcentres.pw',
'nrod.top',	'postcentres.shop',
'omniva.top',	'postcolombia.co',
'omnivaee.top',	'postcorihu.top',
'omnivaee.xyz',	'postcorihu.xyz',
'omnivai.xyz',	'poste-at.top',
'open-rice-serice.top',	'poste-it.services',
'open-rich.top',	'poste-server.top',
'package-tracking.top',	'poste-track.top',
'plpsc.top',	'poste-tracking.top',
'poczta-polska.one',	'poste-tracks.top',
'polskapl.top',	'postea-si.top',
'posindonesia.top',	'postea-track.top',
'posnaf.top',	'poster-track.xyz',
'post-ag.live',	'postifi.life',
'post-at.art',	'postifi.top',
'post-en.top',	'postkl.top',
'post-hr.top',	'postlu.life',
'post-news.top',	'postnl.cyou',
'post-office.life',	'postnord-se.xyz',
'post-server.top',	'postnord.store',
'post-t.ink',	'postnorddk-top.top',
'post-t.wiki',	'postof.top',
'post-track-at.top',	'postoffice-za.club',
'posta-hr.co',	'postoffice.lol',
'posta-hr.top',	'postofficeco.one',
'posta-hu.xyz',	'postpy.io',
'posta-romana.vip',	'posts.cyou',
'posta-server.top',	'postse.org',
'posta-service.top',	'postslovakia.co',
'posta-tracking.top',	'postta.top',
'posta.cyou',	'postta.xyz',
'posta.wang',	'pposte-it.xyz',
'postag.ws',	'pptchek.top',
'postahr.buzz',	'psza.life',
'postahu.top',	'ptt-govtr.com',
'postalparcel.info',	'ptt-tr.top',

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF

'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'

Autorzy:
Karol Paciorek
Patryk Baryszewski
CSIRT KNF