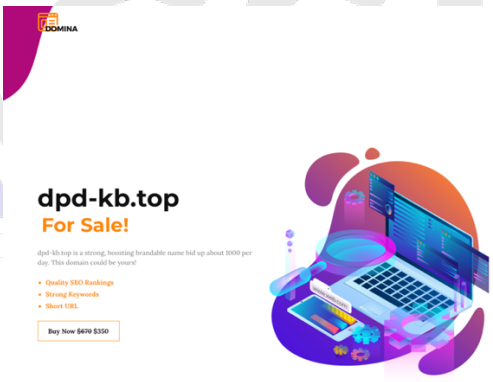
Globalna kampania podszywająca się pod usługi pocztowe

Infrastruktura:

- **Unikalne Domeny**: Zbadane dane zawierają 107 unikalnych domen.
- **Unikalne Adresy IP**: W zestawie danych znajduje się 162 unikalnych adresów IP.
- **Najczęstsze Organizacje AS (liczba wystąpień)**:
  - PACIFICRACK: 79
  - Tencent Building, Kejizhongyi Avenue: 36
  - AS-CHOOPA: 30
  - Kaopu Cloud HK Limited: 19
  - COGENT-174: 9
- **Protokoły**:
  - HTTP: 120 wystąpień
  - HTTPS: 97 wystąpień
- **Tytuł Strony**: Wszystkie strony posiadają jednakowe tytuły – „This domain is for sale.”



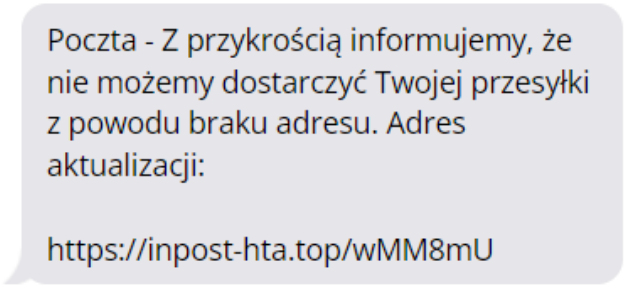
1. Zaślepka - jeden z mechanizmów maskowania stosowany przez przestępców.

Wnioski: Zgromadzone dane wskazują na to, że podmioty stojące za tymi domenami mogą prowadzić działalność phishingową, celując w usługi pocztowe. Użycie jednolitego tytułu i grafiki sugerującej, że domena jest na sprzedaż, może być strategią mającą na celu zmylenie analityków cyberbezpieczeństwa i użytkowników końcowych. Fakt, że docelowa strona pokazuje się tylko po podaniu prawidłowego katalogu w adresie URL, dodatkowo potwierdza podejrzany charakter tych domen. Wysoka koncentracja domen wśród określonych organizacji AS może sugerować, że te organizacje są bardziej podatne na wykorzystanie przez oszustów lub nieświadomie stają się częścią infrastruktury wykorzystywanej do phishingu.

KAROL PACIOREK
PATRYK BARYSZEWSKI

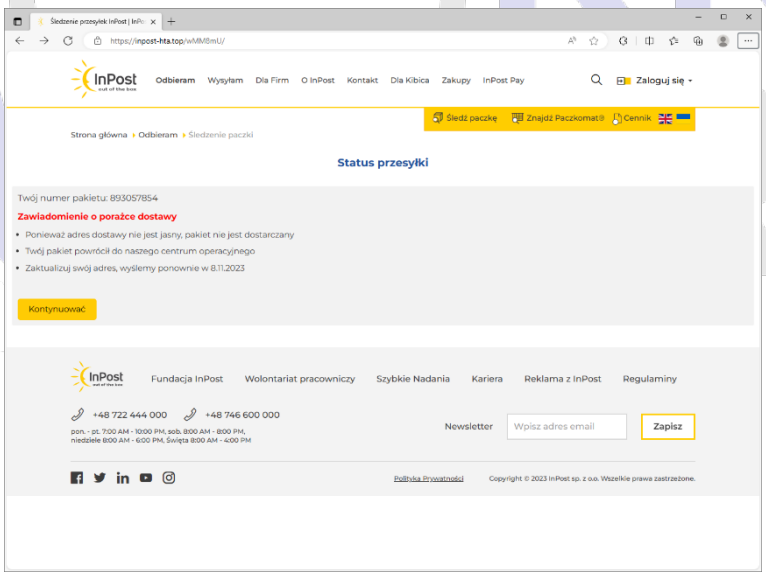
Atak phishingowy:

Cyberprzestępcy wykorzystują wiadomości SMS do dystrybucji fałszywych stron:



2. Przykładowa wiadomość SMS rozsyłana w Polsce.

SMS zawiera bezpośredni adres URL, wraz z katalogiem, pod którym wyświetlana jest fałszywa strona podszywająca się pod firmę Inpost. Po kliknięciu w link ofiara zostaje przeniesiona na stronę phishingową, gdzie w dalszych krokach wykradane są dane osobowe oraz dane karty płatniczej:



3. Fałszywa strona podszywająca się pod Inpost.

Cyberprzestępcy generują katalogi i ścieżki URL w sposób losowy lub zautomatyzowany, co znacznie utrudnia szybkie identyfikowanie i blokowanie domen przez analityków cyberbezpieczeństwa. W przypadku bezpośredniego wejścia na domenę wyświetla się zaślepka (rys. 1).

Przykładowe katalogi, zidentyfikowane w ramach działalności kampanii phishingowej:

- /Fe225w/
- /by4fsL/
- /uFQCqc/
- /Sp1on/
- /kOalVz/
- /LzE2Px/
- /X0aHAM/
- /Ue9Ml8/
- /SQLMqv/
- /OpxZY4/
- /HajsyZ/
- /XSckUl/
- /yxS2XZ/

Generowane katalogi, przyjmują struktury zawierające od 5 do 6 znaków, składają się z małych i dużych liter oraz cyfr, tworząc zestawienie o wysokiej entropii, które stanowi wyzwanie w detekcji i analizie dla ekspertów cyberbezpieczeństwa.

W celu dalszego utrudnienia detekcji, cyberprzestępcy implementują również mechanizmy rozpoznawania geolokalizacji użytkownika. Przy pomocy tego rozwiązania, dostęp do pełnej zawartości sfałszowanej strony phishingowej jest możliwy wyłącznie po połączeniu z IP zlokalizowanym w kraju docelowym kampanii. W sytuacji, gdy próba dostępu do strony zostanie podjęta z adresu IP poza ustalonym obszarem geograficznym, użytkownikowi prezentowana jest zaślepka informująca o możliwości zakupu domeny (rys. 1).

Dodatkowym elementem strategii zabezpieczeń stosowanych przez cyberprzestępców jest weryfikacja pola User-Agent w nagłówku zapytania HTTP. To pole służy jako identyfikator typu urządzenia, z którego dokonywane jest połączenie. Pełna zawartość sfałszowanej strony jest udostępniana wyłącznie wtedy, gdy zapytanie pochodzi z urządzenia mobilnego – stwierdzone to jest na podstawie mobilnego User-Agenta. Jeśli wykryty zostaje User-Agent wskazujący na przeglądarkę desktopową, zamiast złośliwej strony wyświetlona zostanie zaślepka (rys. 1).

Podobną kampanię o takiej skali mogliśmy zaobserwować w Lipcu 2023 roku. Raport, gdzie opisaliśmy ww. atak na klientów usług pocztowych znajduje się poniżej:

Język Polski:

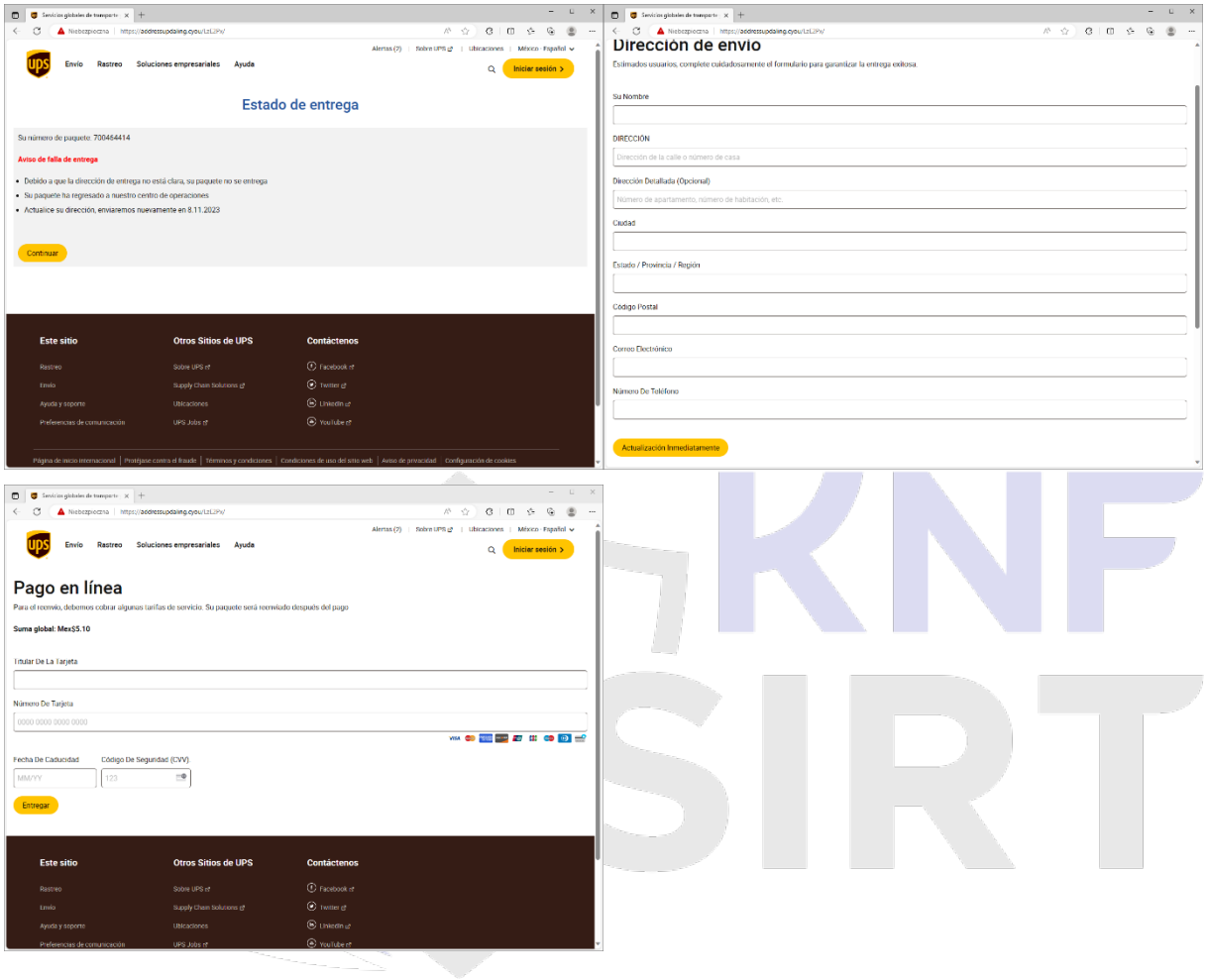
https://cebrf.knf.gov.pl/images/Midzynarodowa_Kampania_Phishingowa_PL-2_1.pdf

Język Angielski:

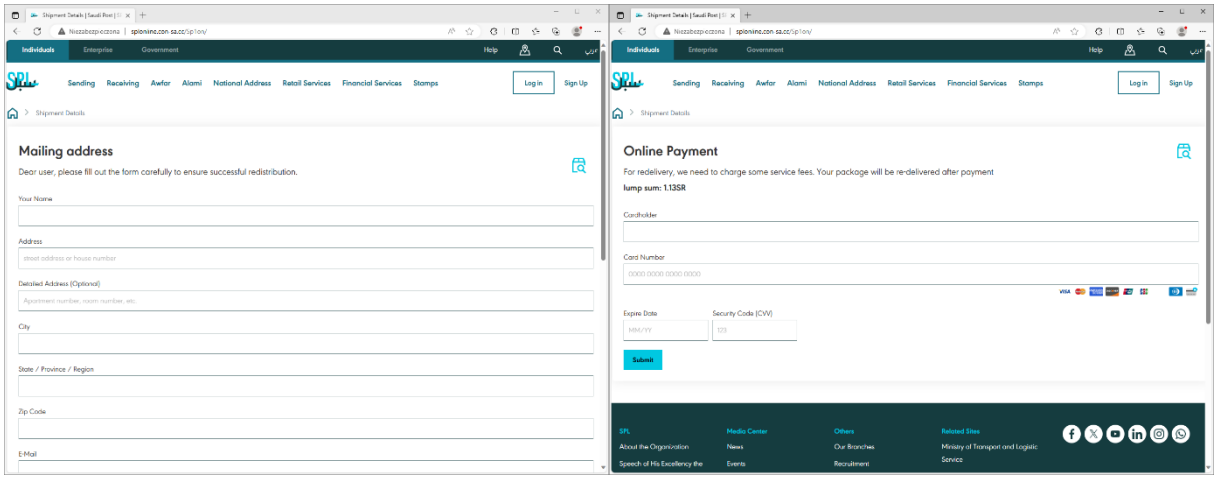
https://cebrf.knf.gov.pl/images/International_phishing_campaign_EN-2.pdf

Przykłady stron phishingowych zidentyfikowane w innych krajach:

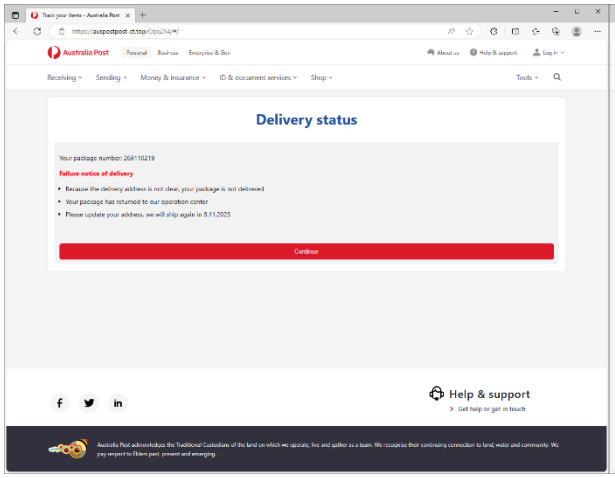
Meksyk:

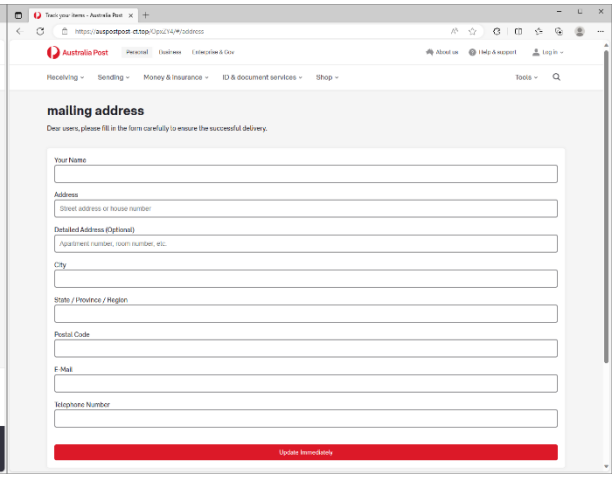


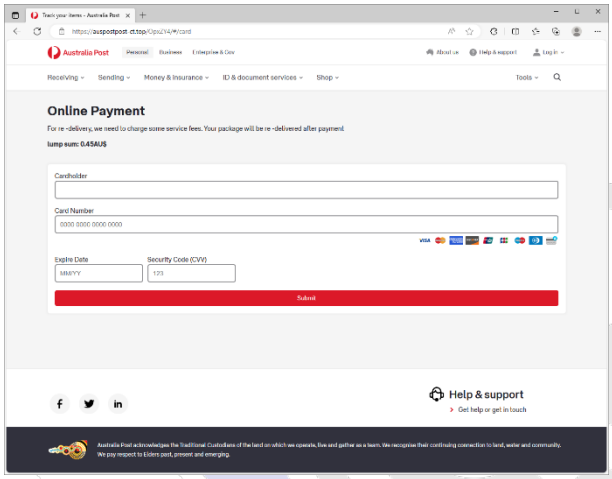
Arabia Saudyjska:



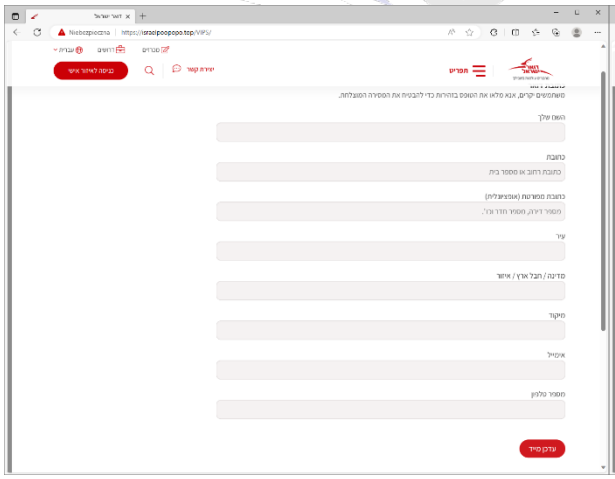
Australia:

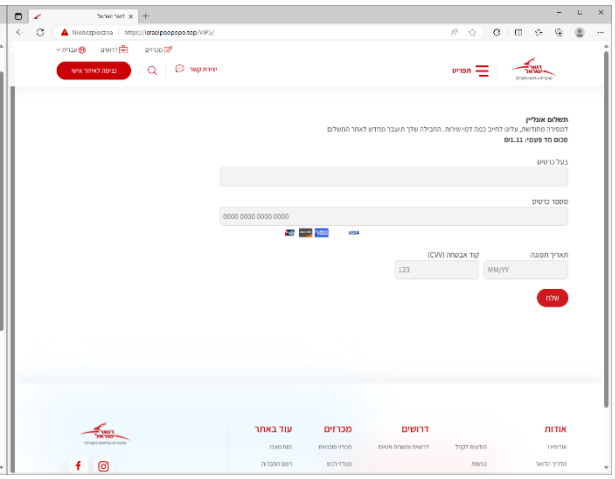




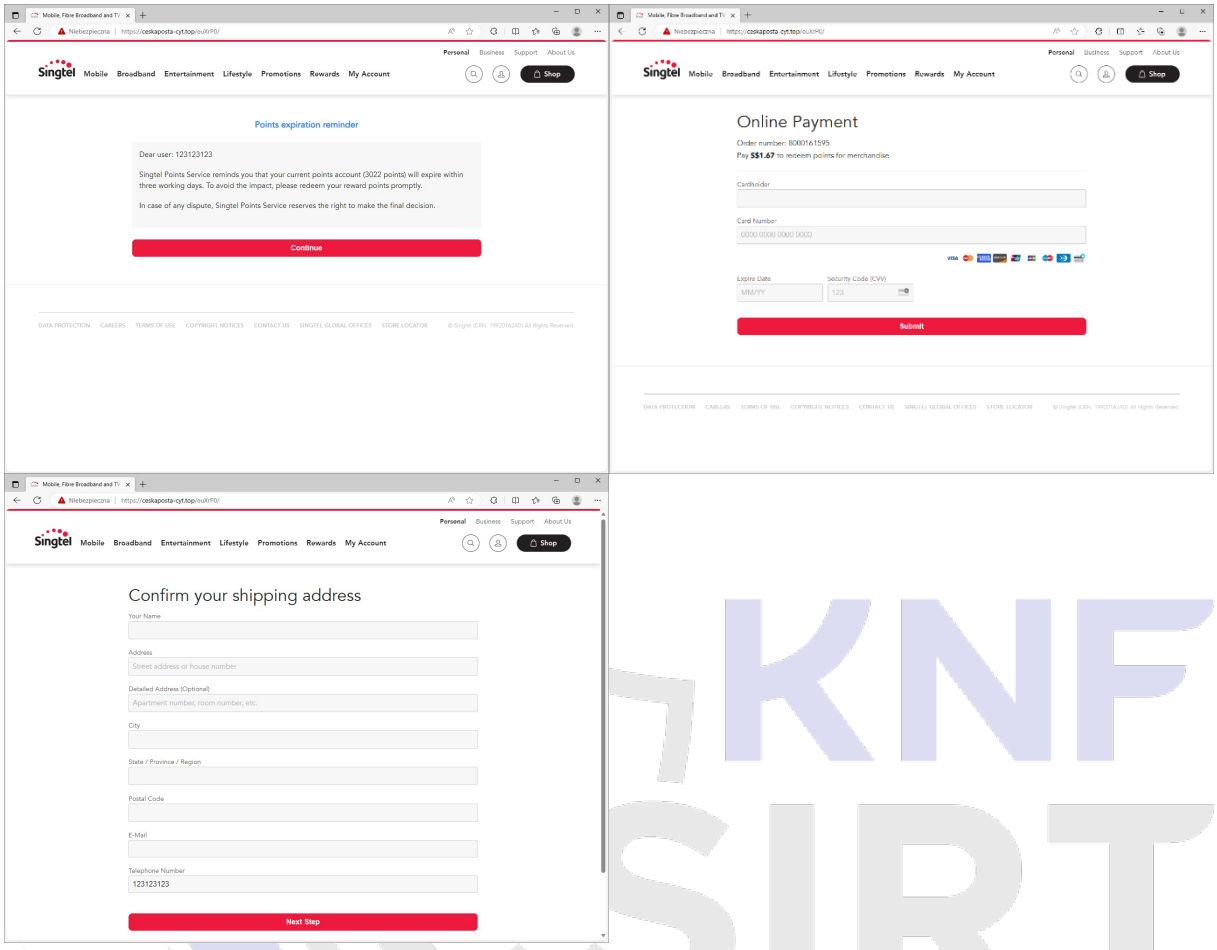


Izrael:

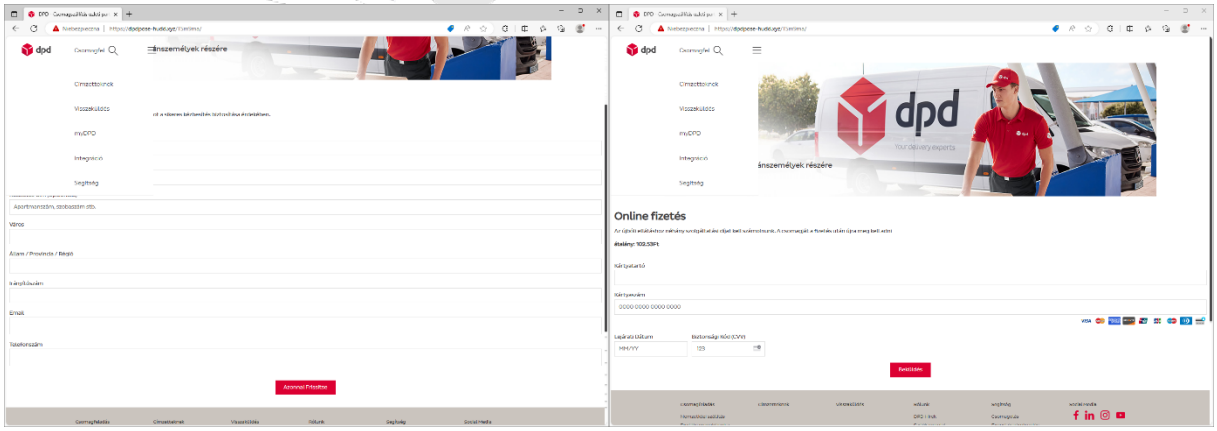




Czechy:



Węgry:



IoC – IPs:

155.94.178.141	38.47.122.55	38.54.104.145	155.94.182.72	45.76.13.238
43.153.79.244	104.223.15.164	155.94.184.231	208.167.242.218	198.52.123.190
45.95.172.118	108.61.229.181	139.84.226.3	155.94.182.55	
38.60.251.246	204.44.66.6	155.94.163.244	155.138.206.250	
43.131.23.250	45.32.87.8	154.23.208.252	155.94.182.56	
43.159.130.175	141.11.137.205	142.171.242.247	155.94.182.68	
107.151.250.75	155.94.184.148	170.106.114.61	38.54.86.38	
104.223.15.216	154.26.192.28	43.130.48.56	207.148.30.199	
104.223.15.16	140.82.46.19	38.60.199.61	155.94.235.40	
155.94.201.164	108.61.147.151	155.94.184.226	155.94.182.42	
139.180.130.123	45.77.200.90	192.227.137.227	155.94.182.38	
194.87.68.241	47.88.13.114	66.103.207.89	136.244.90.36	
155.94.184.178	38.54.119.18	204.44.66.14	155.94.178.152	
104.223.15.26	155.94.184.165	207.148.25.146	155.94.178.164	
155.94.201.194	192.53.120.28	192.248.182.16	155.94.128.9	
43.159.146.211	204.44.94.113	155.94.182.47	107.150.4.171	
104.223.15.20	74.48.78.120	101.32.166.119	155.94.178.251	
43.135.149.241	155.94.128.32	38.54.25.198	155.94.182.15	
204.44.95.109	45.32.88.234	140.82.29.109	155.94.228.95	
170.106.141.40	38.60.205.159	43.153.85.132	155.94.178.186	
91.92.243.110	155.94.235.78	198.44.169.109	155.94.128.37	
170.106.105.178	154.40.48.206	38.54.104.192	155.94.178.177	
155.94.184.150	155.94.184.149	47.251.43.67	159.203.179.90	
155.94.184.209	195.133.53.222	23.94.169.185	104.129.63.6	
154.29.148.35	38.60.196.40	43.130.43.205	204.44.95.60	
43.131.32.99	154.12.93.126	155.94.184.158	155.138.200.171	
154.12.95.11	23.94.169.16	155.94.178.168	38.54.101.211	
107.150.7.34	155.94.184.146	137.220.51.95	38.54.88.62	
170.106.194.39	204.44.66.10	155.94.228.158	155.94.178.155	
38.54.108.74	43.135.185.36	155.94.182.51	204.44.92.102	
204.44.93.192	104.234.25.56	43.153.88.85	155.94.178.148	
43.159.131.234	66.135.23.193	47.91.67.82	155.94.128.10	
155.94.184.161	170.106.153.179	94.156.67.200	155.94.178.151	
155.94.182.21	49.51.180.7	155.94.182.74	38.54.71.124	
104.223.15.207	155.94.184.102	155.94.182.207	165.232.146.81	
45.77.32.110	38.54.101.185	45.32.79.72	45.138.16.207	
66.103.207.162	155.94.128.11	155.94.182.215	204.44.92.224	
142.171.185.171	38.54.110.199	104.238.129.96	45.77.95.249	
149.28.225.47	154.223.16.151	38.54.101.183	108.61.73.152	
155.94.184.250	149.28.138.191	38.60.206.85	45.77.198.19	

IoC - Domeny:

dpd-kb.top
upaddressluofei.shop
canadapost-postscanadaca.top
limoe.buzz
com-uy.cyou
laposteees.online
upsmxe.cyou
pttgov-tr.xyz
post-aui.top
sjppost.top
lt-postlinkt.xyz
postalrule.xyz
depost.cyou
correoswork.cyou
brunei-post.top
twfetcat.xyz
posts-in.top
filan.cyou
singepro.xyz
poastaupota.top
eppgovpk.top
hocdol.top
qatarpostoffice.life
azteca.top
govpostses-tr.top
expro-qatpost.top
post-chde.xyz
supprot-info.icu
postamd.top
us-re.cyou
telkomselus.top
transitevents.top
aukuaidi-post.shop
singpostoffice.com
azteca2.top
hkd.skin
postalfix.info
poste1.icu
jordanpost-nbx.top
ceskaposta-utz.top
postheasconsulting.top
singxepost.bond
taiwamnobile.pics
gobpeserposn.cyou
post-dh.top
coles-cmj.top
upsmxx.cyou
gobpeserpost.online
singposta-sg.top
sg-post-t.life
postxu.top
tollbillpay.top
ups365.top
uspsvip123.top
uspslis.top
upscommxeshomepage.online
uspsp.xyz
ckaposts.top
points-xjk.top
mocgoevkw.top
ptt168.top
sing-post-com.top
posts-ksj.top
expro-omepost.top
postacmis.top
trackingcorreosgobbo.online
jrpos.top
hotaimotor-tw.top
xinsuiduan.top
taiwanmobiln.cyou
correuy.top
royalmailcomtrack-your-item.online
postat.site
correosytelegrafoscivgobgt.online
upsmbb.cyou
sgpose.xyz
upsmxc.cyou
singpostcom.online
myfoneilg.lat
atpotsi.cyou
royalmailvip.top
correopost.buzz
usps-zok.top
kswshotai.top
dpdposts.top
postjwr.top
usps-top.life
nestwyq.cyou
taiwanmobi.shop
postabschuss.info
sinpgots.top
cazpostt.xyz
correosworkmx.icu
mex-usp.xyz
mxcorreosdemexicogob.online
singtel.website
omnniva-ee.top
singpost-tyz.top
post-oer.com
correo-post.xyz
singapmt.top
delivery9-sg.top
linktlau.info
thepostat.cyou
thepostat.top
post-at.services
rozabg.com