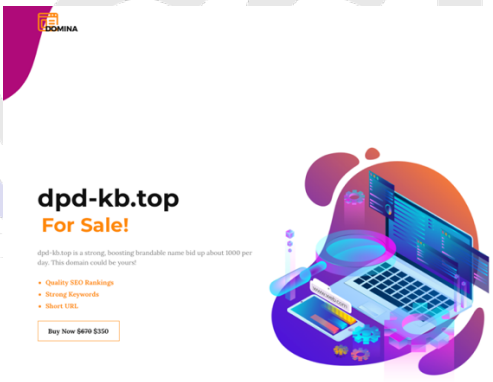
Global campaign impersonating postal services

Infrastructure:

- **Unique Domains**: The data examined includes 107 unique domains.
- **Unique IP Addresses**: there are 162 unique IP addresses in the data set.
- **Most Frequent AS Organizations (number of occurrences)**:
  - PACIFICRACK: 79
  - Tencent Building, Kejizhongyi Avenue: 36
  - AS-CHOOPA: 30
  - Kaopu Cloud HK Limited: 19
  - COGENT-174: 9
- **Protocols**:
  - HTTP: 120 occurrences
  - HTTPS: 97 occurrences
- **Site Title**: All pages have identical titles - "This domain is for sale."



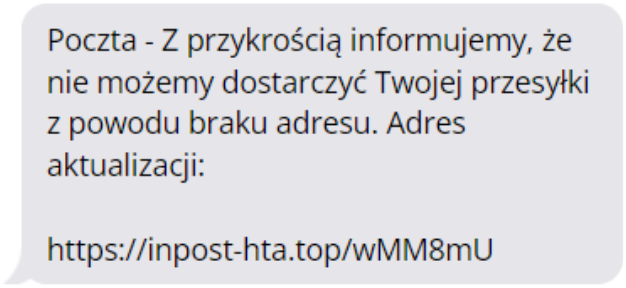
1. Blinding - one of the cloaking mechanisms used by criminals.

Conclusions: The data collected suggests that the entities behind these domains may be conducting phishing activities, targeting email services. The use of a uniform title and graphics suggesting that the domain is for sale may be a strategy to confuse cyber security analysts and end users. The fact that the target site only shows up when a valid directory is specified in the URL further confirms the suspicious nature of these domains. The high concentration of domains among specific AS organizations may suggest that these organizations are more susceptible to exploitation by fraudsters or unknowingly become part of the infrastructure used for phishing.

KAROL PACIOREK
PATRYK BARYSZEWSKI

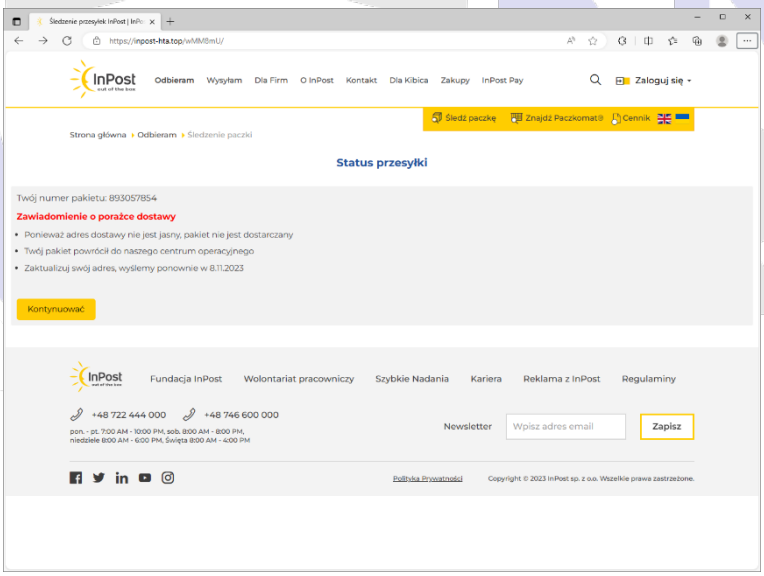
Phishing attack:

Cybercriminals use SMS messages to distribute fake sites:



2. An example of an SMS message distributed in Poland.

The SMS contains a direct URL, along with a directory, under which a fake website impersonating Inpost is displayed. After clicking on the link, the victim is taken to the phishing site, where personal and payment card data are stolen in further steps:



3. A fake website impersonating Inpost.

Cybercriminals generate directories and URL paths in a random or automated manner, making it much more difficult for cyber security analysts to quickly identify and block domains. If a domain is accessed directly, a blanking screen is displayed (Figure 1).

Examples of directories identified by phishing campaign activity:

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

The generated directories, take structures of 5 to 6 characters, consist of lowercase and uppercase letters and numbers, creating a high-entropy juxtaposition that poses a challenge in detection and analysis for cyber security experts.

To make detection even more difficult, cybercriminals also implement mechanisms to recognize the user's geolocation. With this solution, access to the full content of a fake phishing site is possible only when connected to an IP located in the target country of the campaign. In a situation where the site is attempted to be accessed from an IP address outside the established geographic area, the user is presented with a plug-in informing them that they can purchase the domain (Figure 1).

An additional element of the security strategy used by cybercriminals is the verification of the User-Agent field in the HTTP request header. This field serves as an identifier of the type of device from which the connection is made. The full content of the fake page is only made available if the request comes from a mobile device - this is determined by the mobile User-Agent. If a User-Agent pointing to a desktop browser is detected, a blank is displayed instead of the malicious page (Figure 1).

We could see a similar campaign of this scale in July 2023. The report where we described the aforementioned attack on postal service customers is below:

Polish Language:

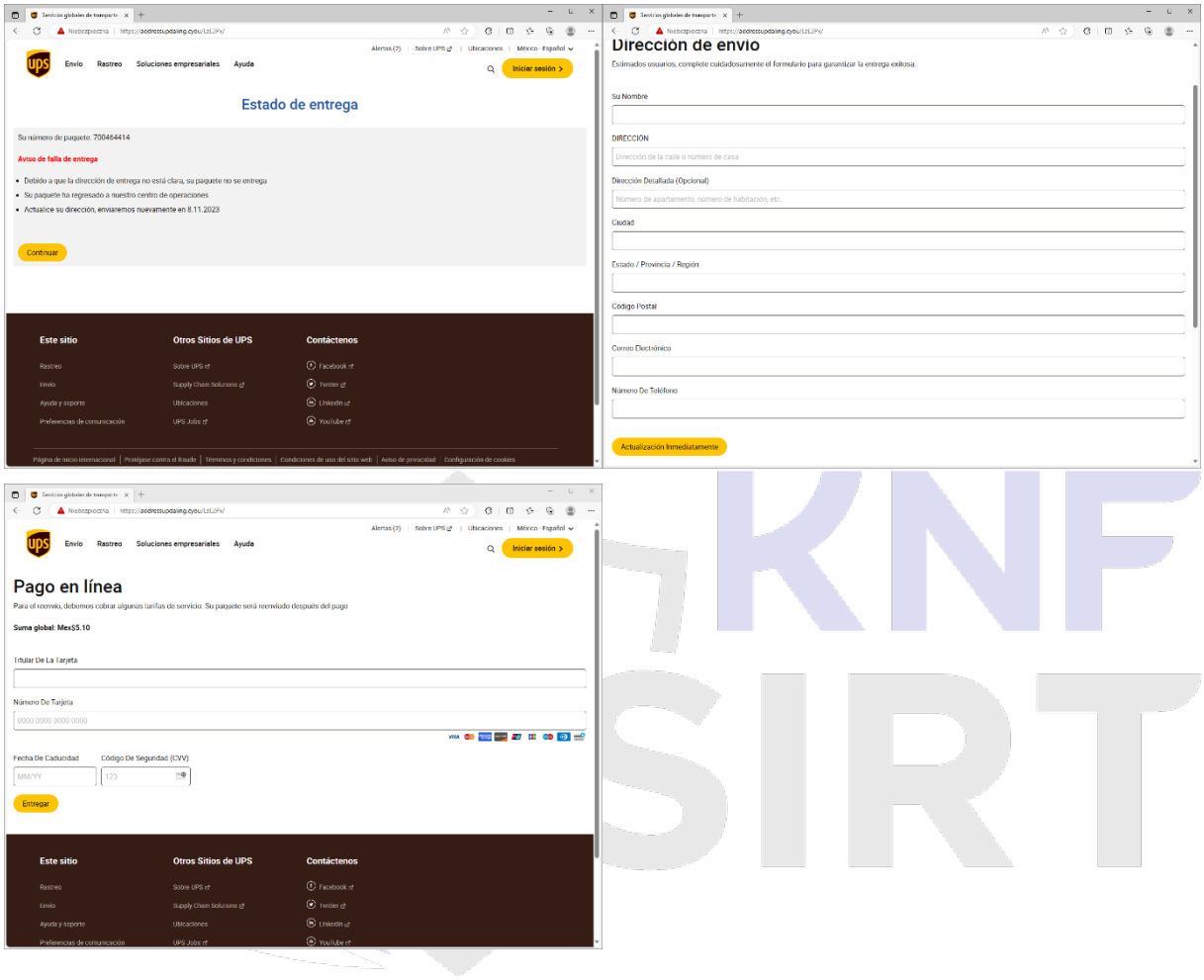
https://cebrf.knf.gov.pl/images/Midzynarodowa_Kampania_Phishingowa_PL-2_1.pdf

English Language:

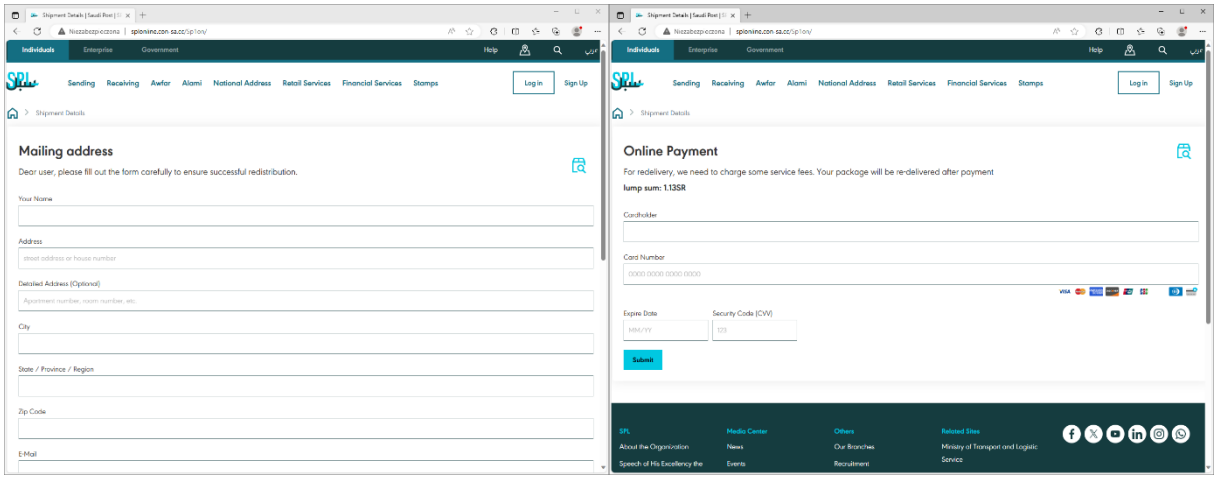
https://cebrf.knf.gov.pl/images/International_phishing_campaign_EN-2.pdf

Examples of phishing sites identified in other countries:

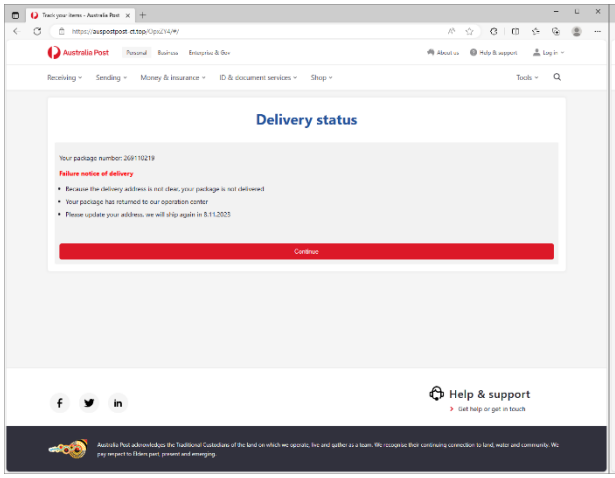
Mexico:

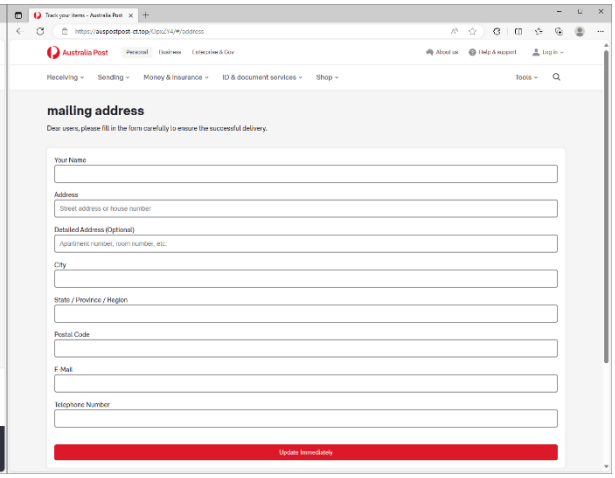


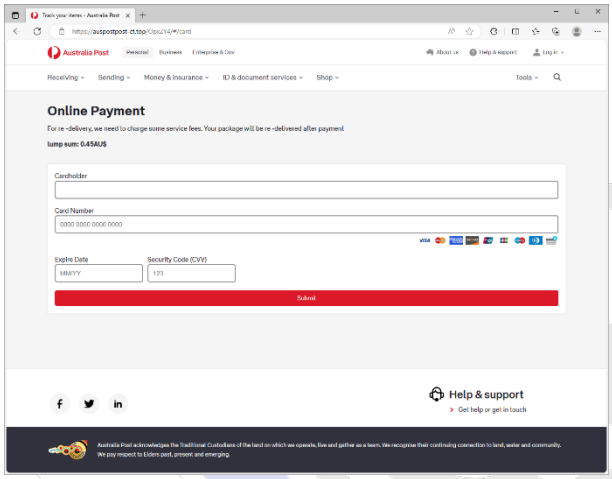
Saudi Arabia:



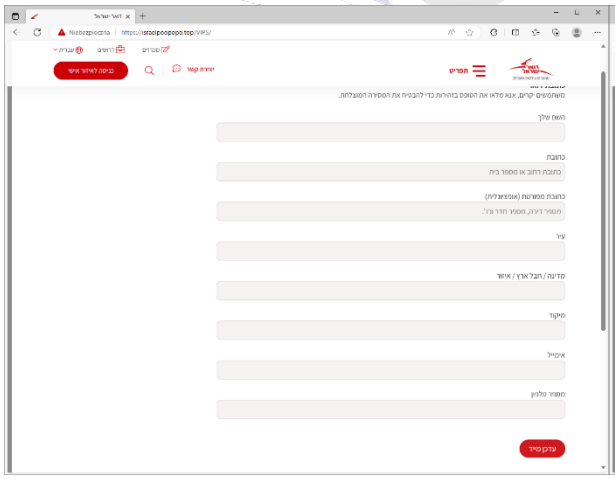
Australia:

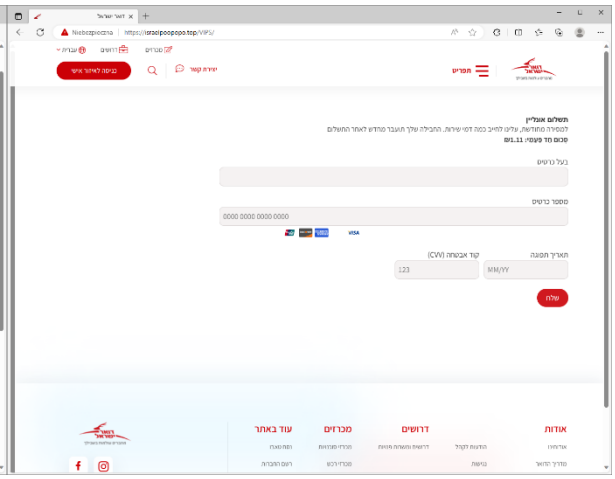




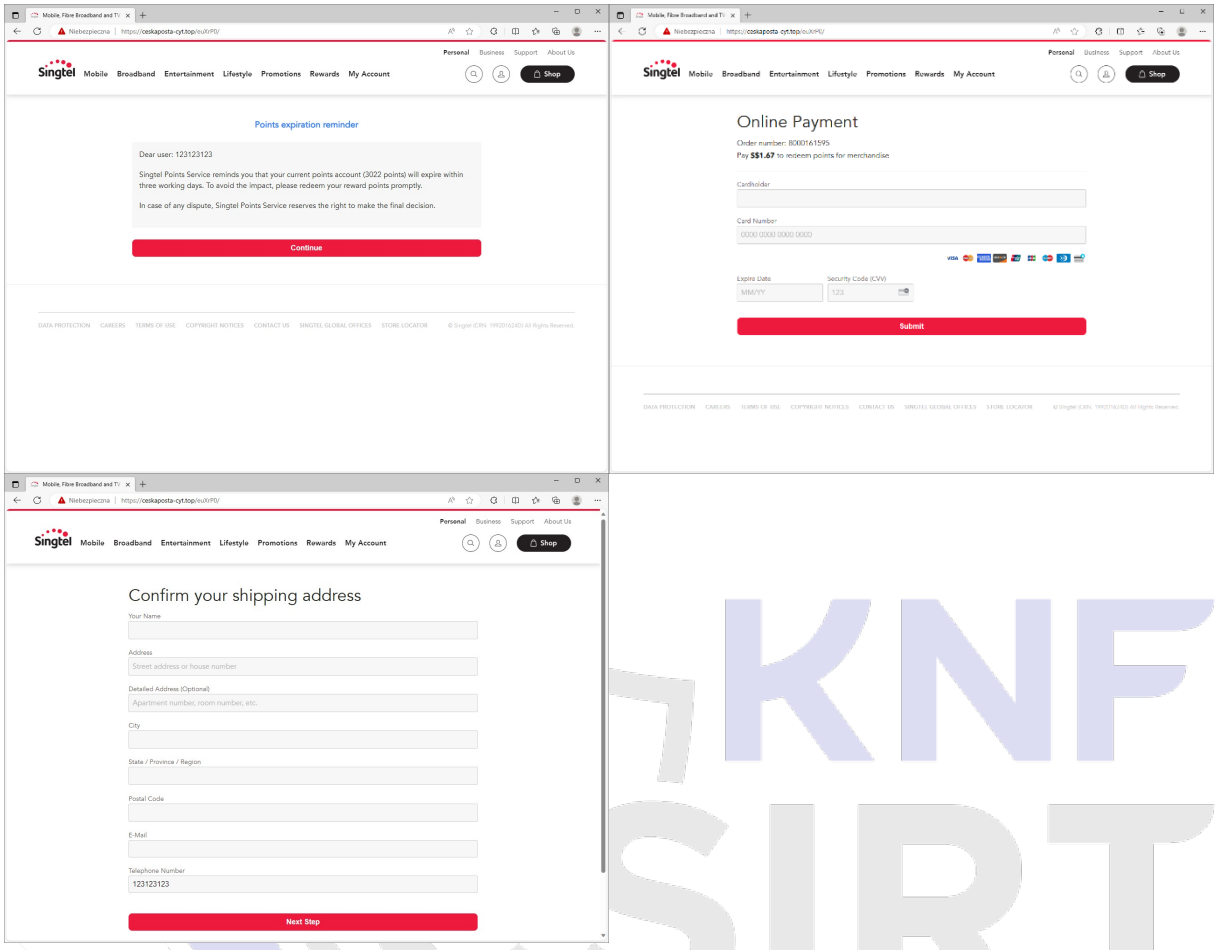


Israel:

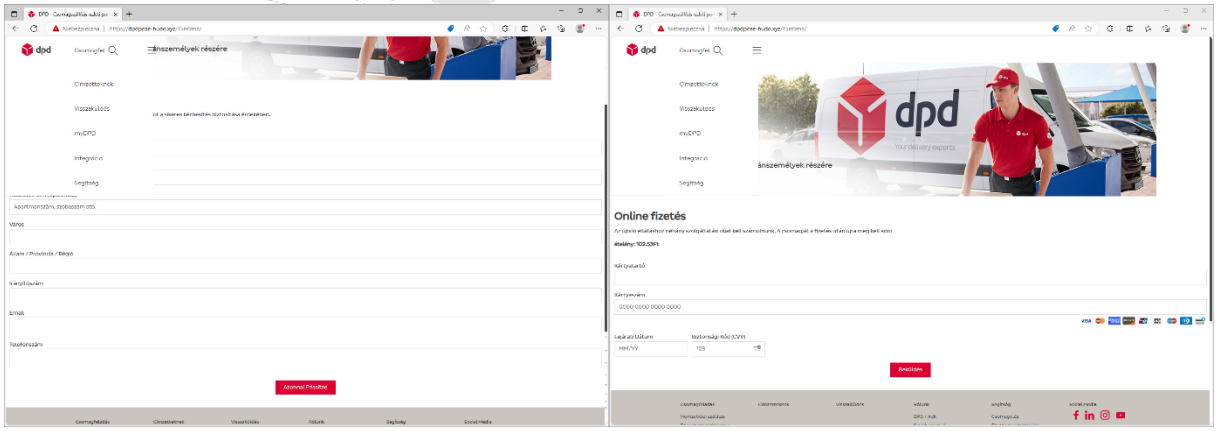




Czech Republic:



Hungary:



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 - Domains:

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-xj.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