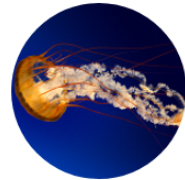


 [github.com/360netlab/DGA/issues/36](https://github.com/360netlab/DGA/issues/36)

360netlab

360netlab/DGA

## #36 From PDNS: Another fix length of 7, a-z. tlds: [ru, com]



 8 comments



**suqitian** opened on May 27, 2017



some new waves are observed recently with **ru** only TLD, all query type **A**. For example, the core domains are like these, detected with very strong correlation, no subdomains:

```
date -u  
Tue Oct 17 22:10:20 UTC 2017
```

```
bhzlyxh.ru.,1  
qsxxzni.ru.,1  
gwjijru.ru.,1  
fyxkmbh.ru.,1  
qwoumzw.ru.,1  
kulfxxy.ru.,1  
nrxboty.ru.,1  
pyjhpx.ru.,1  
qwwzlam.ru.,1  
sbckhnb.ru.,1  
yboqlxs.ru.,1  
qyccsug.ru.,1  
nmtydik.ru.,1  
uzpadrm.ru.,1  
dqoudex.ru.,1  
ssopuyk.ru.,1  
gqlgpob.ru.,1  
fgqjwdl.ru.,1  
tdmxpmi.ru.,1  
rxzyglt.ru.,1  
qmwekpe.ru.,1  
reczrhm.ru.,1  
diacfxa.ru.,1  
neffcrf.ru.,1  
qhrywlc.ru.,1  
hmiwbxq.ru.,1  
wyudsya.ru.,1  
lyfsnwj.ru.,1  
kmgcsug.ru.,1
```

meanwhile, the **wasyellowindexhotel.ru** has many new FQDNs like **w1.wasyellowindexhotel.ru** **w17.wasyellowindexhotel.ru** **w18.wasyellowindexhotel.ru**. An educated guess can lead to some new variant.