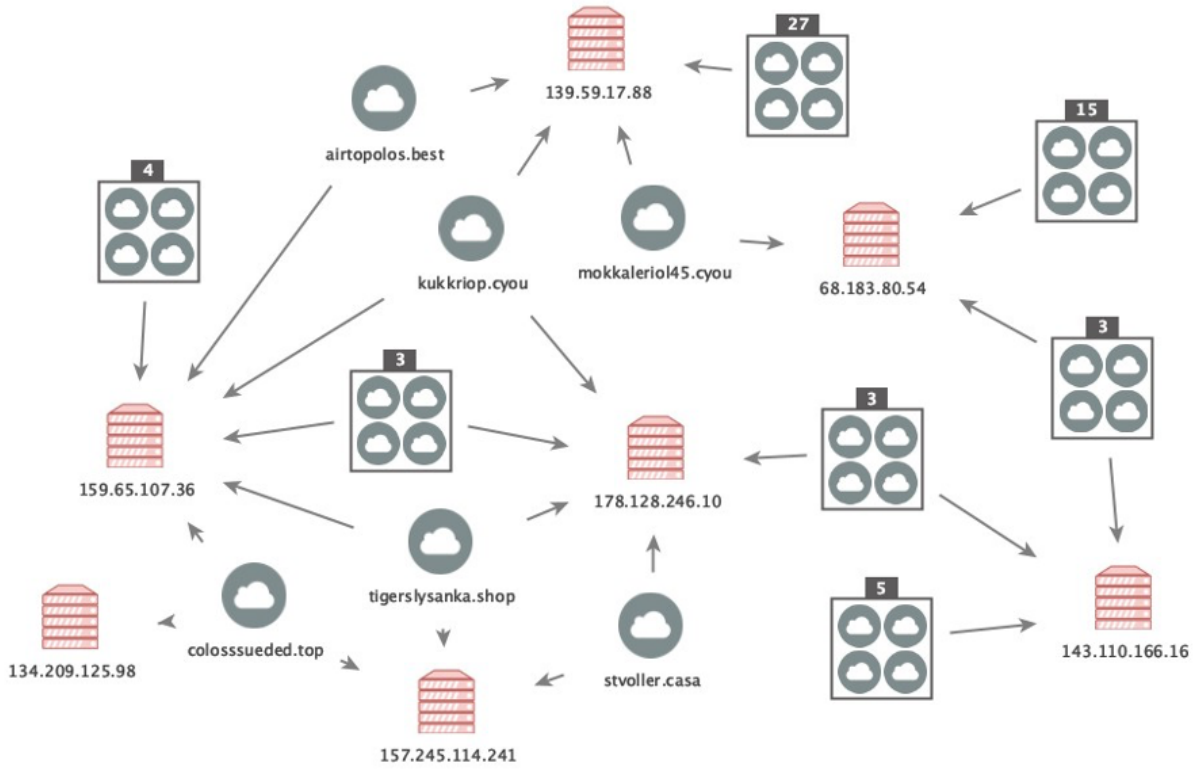
# Tracking BokBot (IcedID) Infrastructure

team-cymru.com/blog/2021/05/19/tracking-bokbot-infrastructure/

S2 Research Team View all posts by S2 Research Team May 19, 2021




**Co-authored by Josh Hopkins, Andy Kraus and Nick Byers**

BokBot (also known as IcedID) started life as a banking trojan using man-in-the-browser attacks to steal credentials from online banking sessions and initiate fraudulent transactions. Over time, the operator(s) of BokBot have also developed its use as a delivery mechanism for other malware, in particular ransomware.

In the past BokBot was itself primarily distributed via the Emotet botnet. Since the takedown of Emotet earlier this year we have been tracking BokBot to see how the actors might react to and seek to exploit the situation for personal gain.

Over recent months we have been posting BokBot IOCs to our Twitter account (@teamcymru_S2) as we identify them. However, in this blog we want to share some of our broader techniques, as well as a brief insight into our recent view of the upward management of BokBot infrastructure. All 'Tier 1' BokBot domains and hosting IP addresses, which we have identified over the past six months, are available through our public GitHub.

Passive DNS

Our research started with a list of BokBot controller domains, identified in a blog post by FireEye in February:

colombosuede[.]club
colosssueded[.]top
golddisco[.]top
june85[.]cyou

Pivoting on these domain names within our Passive DNS (PDNS) data holdings, we were able to identify several dozen linked domains, as well as a handful of 'Tier 1' hosting IP addresses. A summary of these findings is illustrated in Figure 1 below.

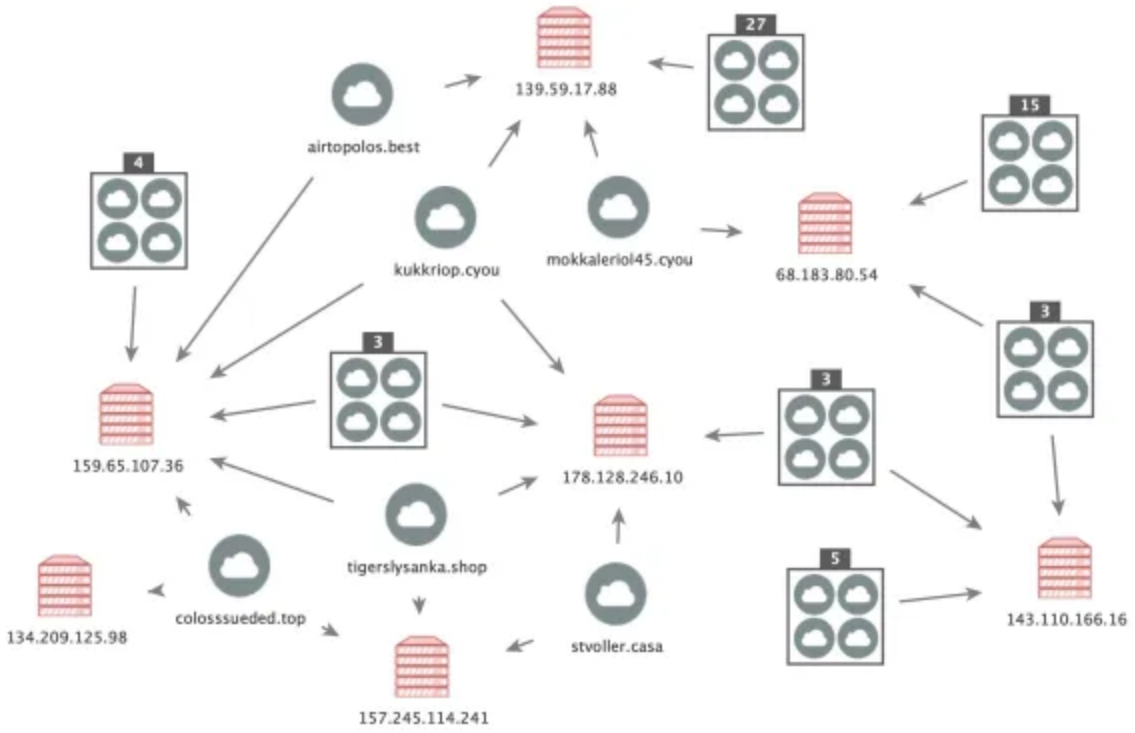



Figure 1: Initial PDNS Pivots

All of the domains we identified in this process used relatively uncommon top-level domains (TLDs) (Figure 2) and were registered through domain name registrars NameSilo and Porkbun. The majority of the Tier 1 IP addresses we identified were assigned to either Digital Ocean or M247.

These three elements (TLD, domain registrar and hosting provider) provide us with a repeating pattern, which gives us a degree of confidence that the identified domains are related.


Figure 2: Most Frequently Occurring TLDs

### Certificate and Banner Information

Looking more closely at the Tier 1 IP addresses hosting these domains, more patterns begin to emerge. Firstly, these IP addresses host a self-signed X.509 certificate with the subject:

CN=localhost, C=AU, ST=Some State, O=Internet Widgits Pty Ltd

Whilst not unique to BokBot hosts, the repeated appearance of this certificate provides another indication that identified infrastructure is linked.

Secondly, we often observed banner information on these IP addresses indicating the use of OpenResty (a web platform based on Nginx). OpenResty has previously been identified as a tool favoured by the BokBot operator(s) for management activities – dating back to 2017.

### Network Traffic Analysis

Next, we utilized our network traffic data holdings to look for common peers amongst the Tier 1 IP addresses. Using this methodology, we identified several Tier 2 IP addresses which were used to relay traffic from the Tier 1 IP addresses over TCP/443. The Tier 2 IP addresses hosted banner information indicating the use of OpenResty, similar to the Tier 1 IP addresses.

We subsequently discovered these Tier 2 IP addresses were exchanging network traffic with dozens of previously unknown Tier 1 IP addresses, which we then enriched with PDNS data to identify further BokBot domains. This process becomes repeatable – pivoting between network traffic and PDNS data until all ‘new’ infrastructure identifications are exhausted.

A common attribute amongst the Tier 2 IP addresses was the hosting of an X.509 certificate with a CN value of ‘main.info’. This certificate was first observed on IP 185.103.110.172, assigned to Creanova Hosting Solutions Ltd in Finland, and subsequently observed on a further sixteen Tier 2 IP addresses (Table 1).

| IP Address | Cert CN | ASN | Geolocation |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 5.101.0.243 | main.info | PINDC | Russia |
| 5.101.0.245 | main.info | PINDC | Russia |
| 31.184.192.39 | main.info | PINDC | Russia |
| 31.184.193.142 | main.info | PINDC | Russia |
| 31.184.193.17 | main.info | PINDC | Russia |
| 46.30.42.185 | main.info | EUROBYTE | Russia |
| 80.66.83.166 | main.info | TRUENETWORK | Poland |
| 185.186.141.140 | main.info | ASKONTEL | Russia |
| 176.9.19.209 | main.info | HETZNER | Germany |
| 45.128.151.15 | main.info | ITL-LV | Latvia |
| 146.185.215.18 | main.info | GCORE | Russia |
| 95.215.0.211 | main.info | PINDC | Russia |
| 45.143.138.72 | main.info | GARANT-PARK-INTERNET | Russia |
| 195.19.192.49 | main.info | DCE-AS | Russia |
| 95.217.51.27 | main.info | HETZNER | Finland |
| 185.18.54.134 | main.info | WORLDSTREAM | Spain |

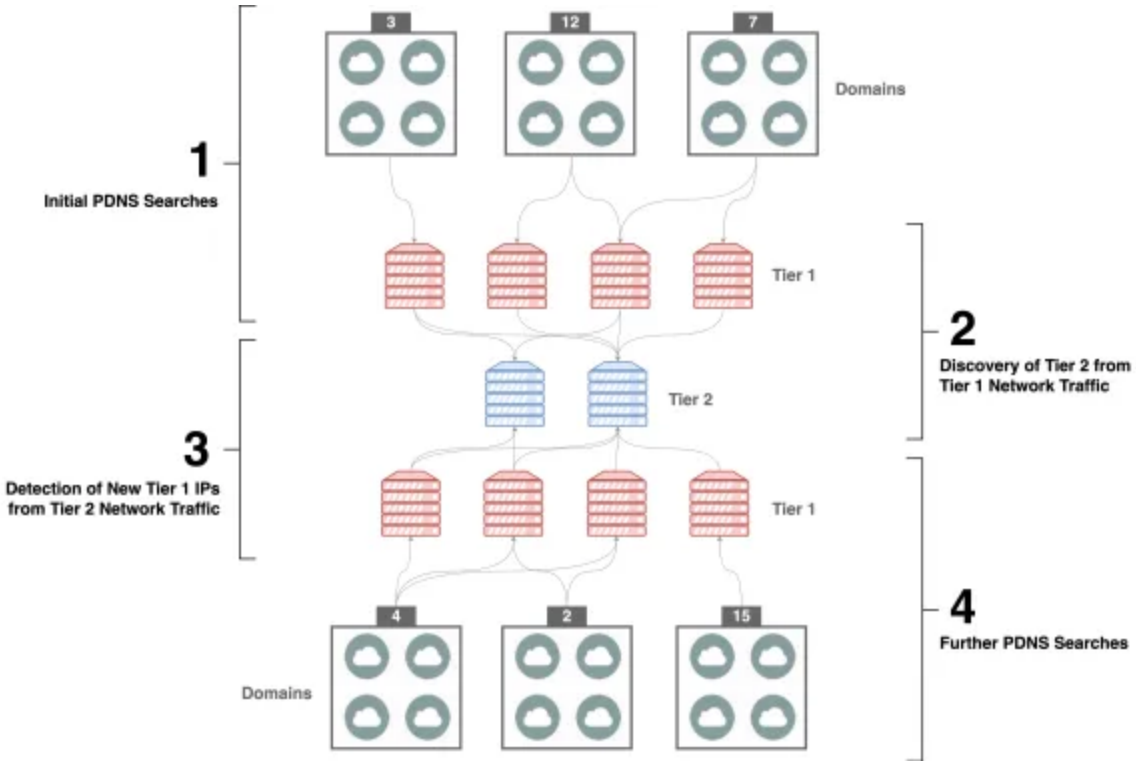



Figure 3: BokBot Infrastructure Discovery Process

We observed the Tier 2 IP addresses in Table 1 being used in the management of BokBot infrastructure over a number of months. However, on 29 April 2021 we noticed a significant drop-off in activity, which has remained consistent to the time of publishing (Figure 3).

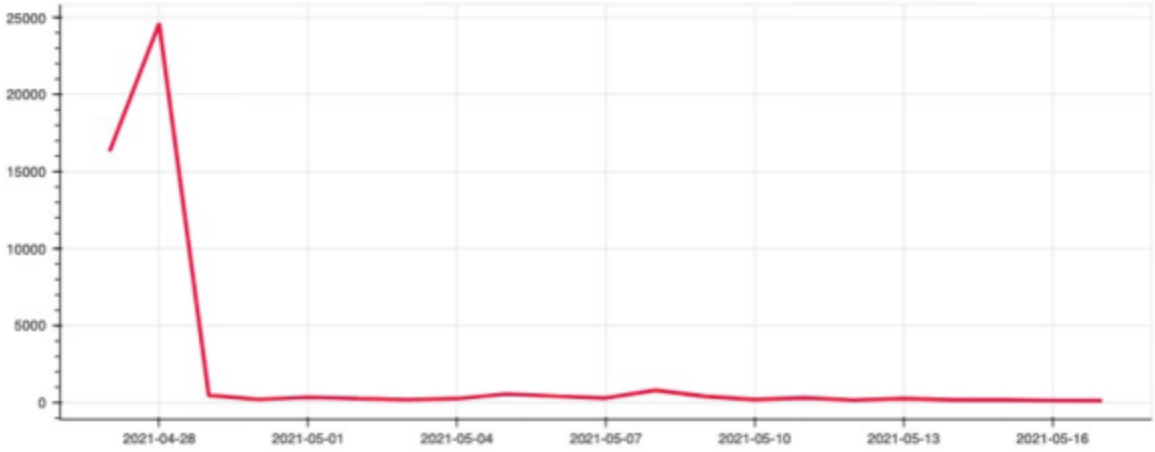



Figure 4: Tier 2 IP Address Activity Timeline

## Conclusion

In conclusion, while BokBot operations may have been temporarily impacted by the Emotet takedown, our analysis shows they are currently running a vast and active network which encompasses upwards of 1,500 domains hosted on over 250 Tier 1 IP addresses.

We hope that the releasing of these indicators proves helpful in identifying and mitigating existing BokBot activities and also in disrupting the future operations of the BokBot actor(s).

Our findings are summarized in Figure 5 below:

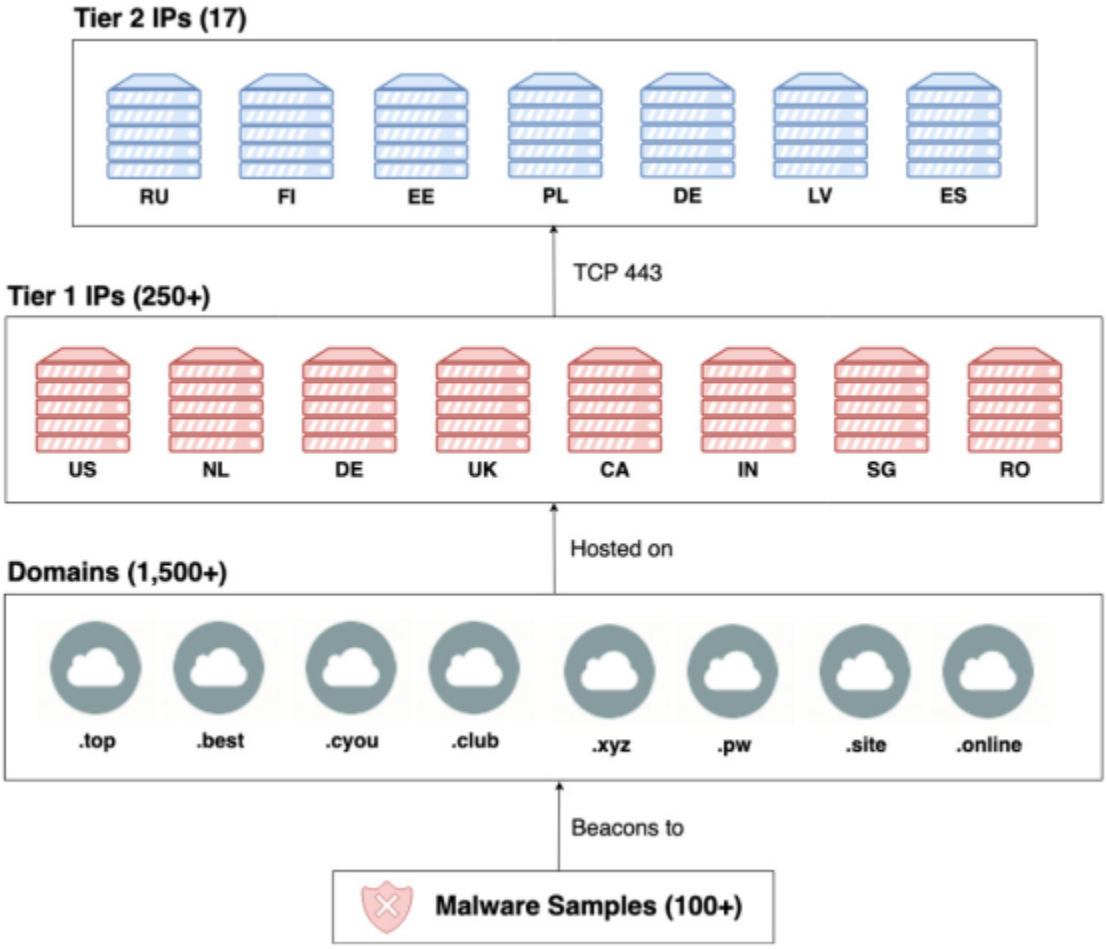



Figure 5: BokBot Infrastructure Overview