Operation DustySky

Clearsky
clearskysec.com/dustysky

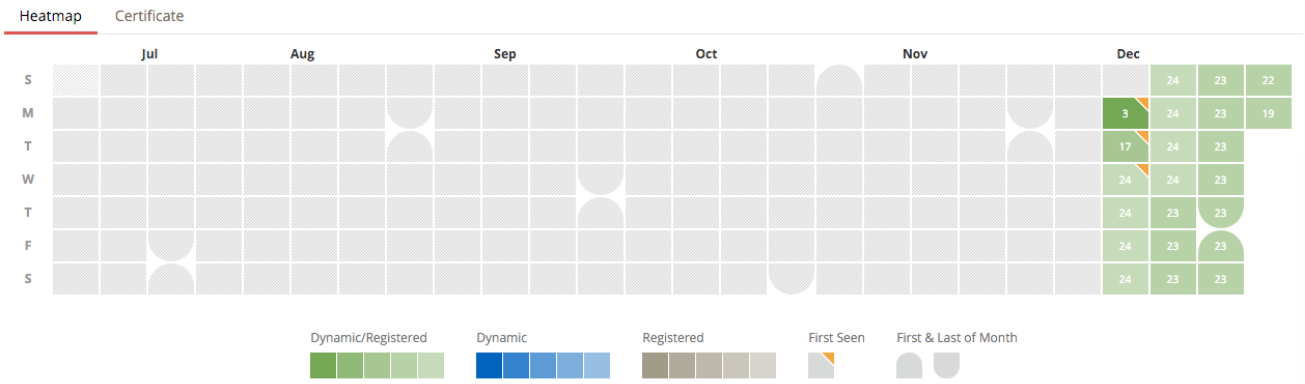
TLP:White
For public distribution

Operation DustySky Notes

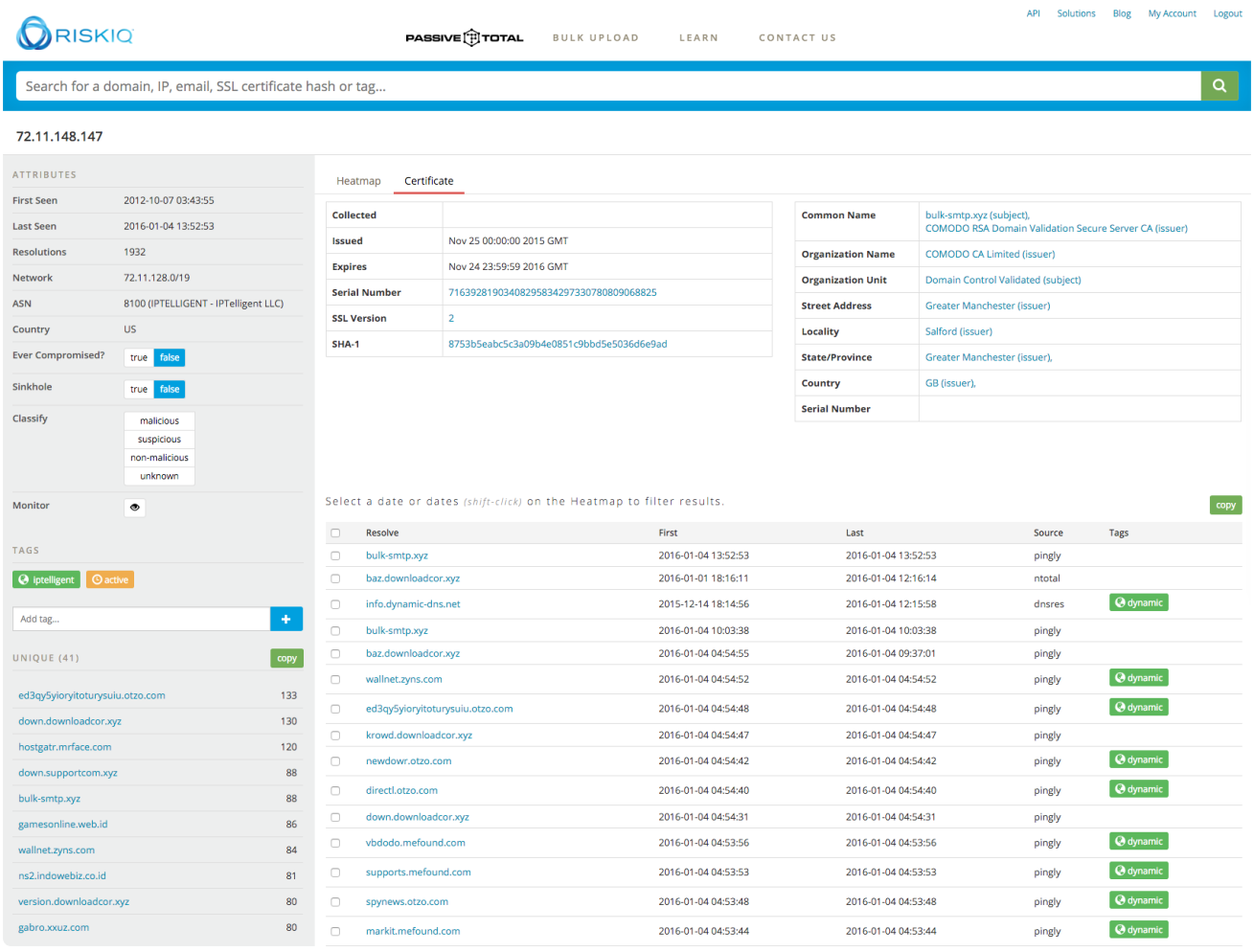
Earlier this morning, Eyal from Clearsky Cyber Security publisheda paper on "Operation DustySky", a set of targeted campaigns attributed back to the Gaza Cybergang. When working with Clearsky, we observed some interesting details and overlap that didn't quite fit in the paper, so we wanted to publish them here.

72.11.148.147

We found this IP address to be interesting due to the SSL certificate, mix of dynamic DNS and registered domains and recent activity.



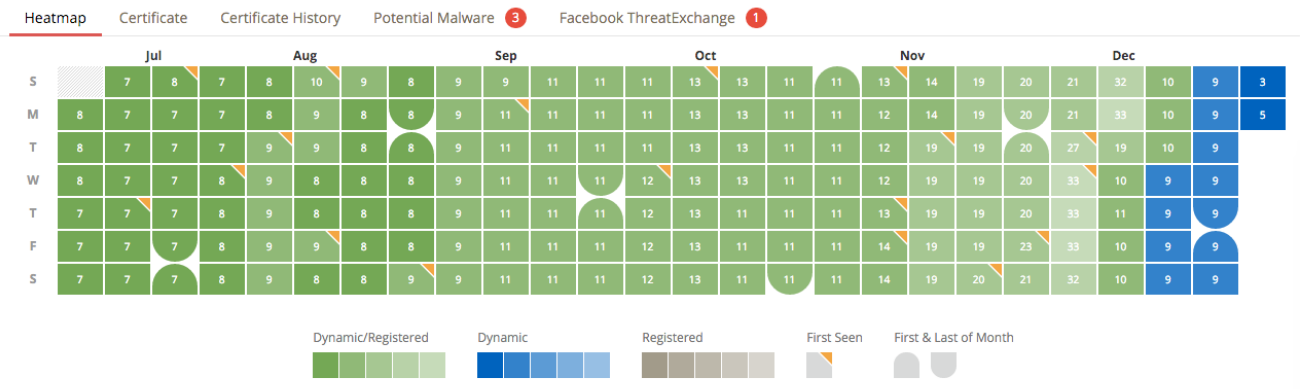
Based on the heatmap above, a user can easily identify that traffic to this particular IP is fairly new (showing in mid-December). What's worth noting is that the first day starts with just one resolution, followed by 17 and then 24. Those first 3 days appears to be significant as newly observed domains (notated by the orange flag) are seen and then it's nothing new over the next few weeks.



The certificate for this domain is interesting, but does not appear to lead to any new discoveries. Clicking on "Serial Number", "Common Name" and "SHA-1" do not reveal anymore new IP discoveries or overlap.

192.161.48.59

This IP address is interesting because of the SSL certificates, but mainly due to some overlap with Gaza Cybergang and a strange pattern in the domain changes.



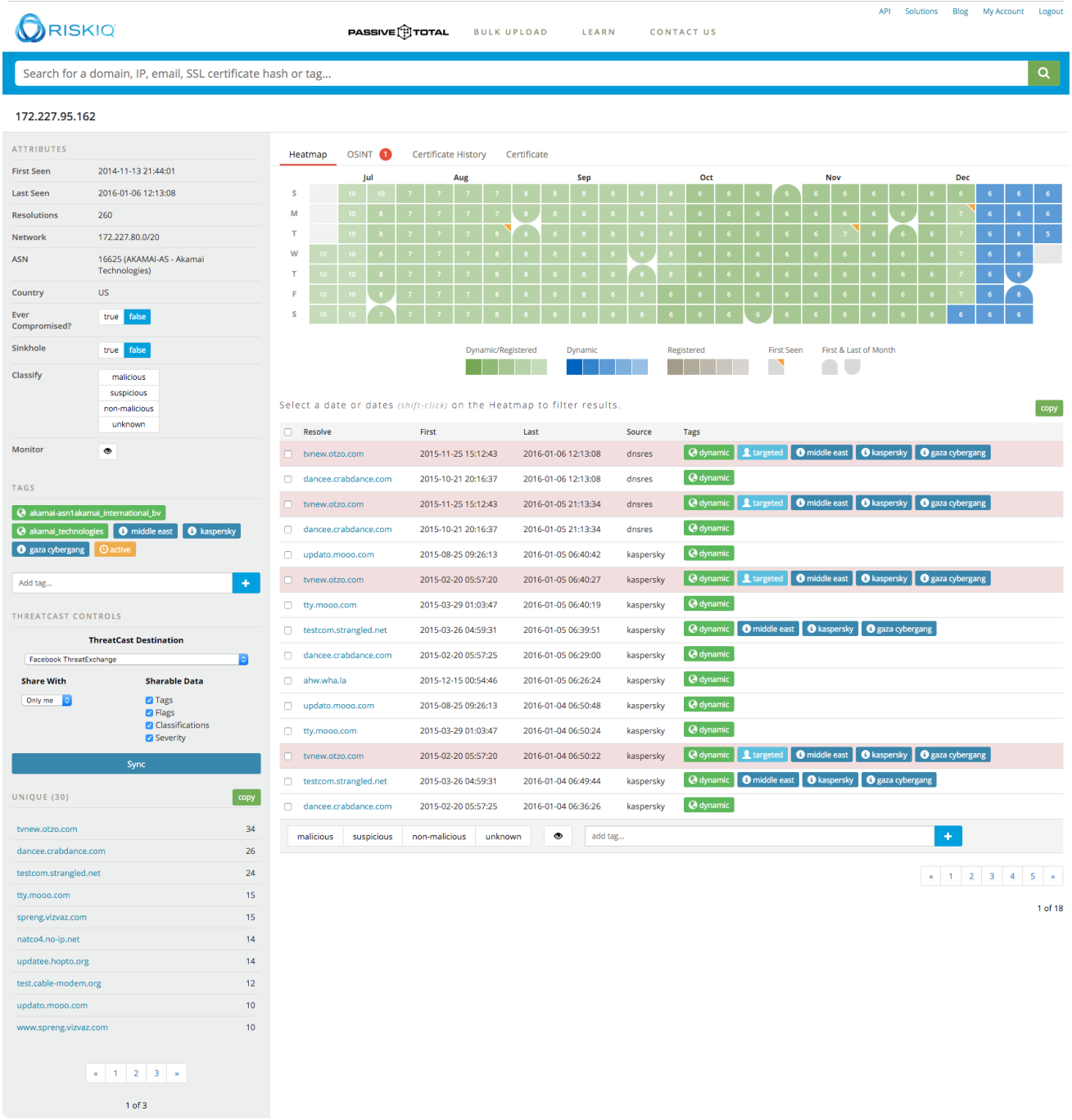
In this heatmap, you can see a clear change from Dynamic/Registered infrastructure to just dynamic infrastructure in the past ~2.5 weeks. While this may not be significant, it's worth noting and should be investigated or compared to attack times. Did attackers stop on the same day they switched to dynamic DNS only? Was this infrastructure used again?

Resolve	Location	Network	First	Last	Source	Tags
185.82.202.207	N/A	185.82.202.0/24	2015-07-29 03:09:26	2016-01-05 22:25:53	mnemonic, pingly, virustotal, kaspersky	hshost_sailor
192.161.48.59	US	192.161.48.0/20	2015-04-30 00:14:14	2015-07-22 04:55:28	riskiq, kaspersky	iptelligent, DustySky
172.227.95.162	US	172.227.80.0/20	2015-04-22 05:00:39	2015-04-22 05:59:47	mnemonic, riskiq	akamai-asn1akamai_international_bv, akamai_technologies, middle east, kaspersky, gaza cybergang
192.161.48.59	US	192.161.48.0/20	2015-04-22 00:00:00	2015-04-22 00:00:00	virustotal	iptelligent, DustySky

Above is a screenshot of the results table from update.ciscofreak.com which used the 192.161.48.59 address back in April of this year. It's worth noting that based on the PassiveTotal OSINT tags, you can see that Kaspersky had reported on the Gaza Cybergang for the IP address 172.227.95.162 which resolved at the same time. While time periods may not overlap completely (was 192.161.48.59 used for malicious purposes in April?), it's still worth investigating.

172.227.95.162

This IP address was reported by Kaspersky as being linked to Gaza Cybergang and shows overlap to the DustySky infrastructure in April of this year. Looking at the results, it's interesting that it seems to show a similar pattern of dynamic/registered domains and then a sudden shift to dynamic DNS only.



The results seem to show more potential links to malicious activity with dynamic DNS domains not mentioned in reporting being shown. Due to the dynamic DNS nature, there's a good chance these are not related or may no longer be malicious, but they still have recent activity that could be used as a research point.

Collected	
Issued	Oct 15 00:00:00 2015 GMT
Expires	Oct 14 23:59:59 2016 GMT
Serial Number	136553595735860340727454403125203608956
SSL Version	2
SHA-1	e03009f07bf799a8d14f7efa0f3467d43773c7d2

Common Name	*.ql.aquire.com.au (subject), GeoTrust SSL CA - G3 (issuer)
Organization Name	QANTAS AIRWAYS LIMITED (subject), GeoTrust Inc. (issuer)
Organization Unit	IT (subject)
Street Address	New South Wales (subject),
Locality	MASCOT (subject),
State/Province	New South Wales (subject)
Country	US (issuer), AU (subject)
Serial Number	

Also, worth showing that there's an SSL certificate associated with the IP address from October of last year. It's a wildcard certificate that shows a relation to Quantas Airways

Limited giving us a timeframe that the current holders appear to be non-malicious and that started around October. Anything before that period could be suspect. Also, it's strange that those Dynamic DNS domains continue to point to the IP despite being owned by a real service. Did the attackers abandon their infrastructure?

45.32.13.169

This IP address shows a connection to the following SSL certificate starting in October of 2015.

Heatmap | Certificate History | Certificate

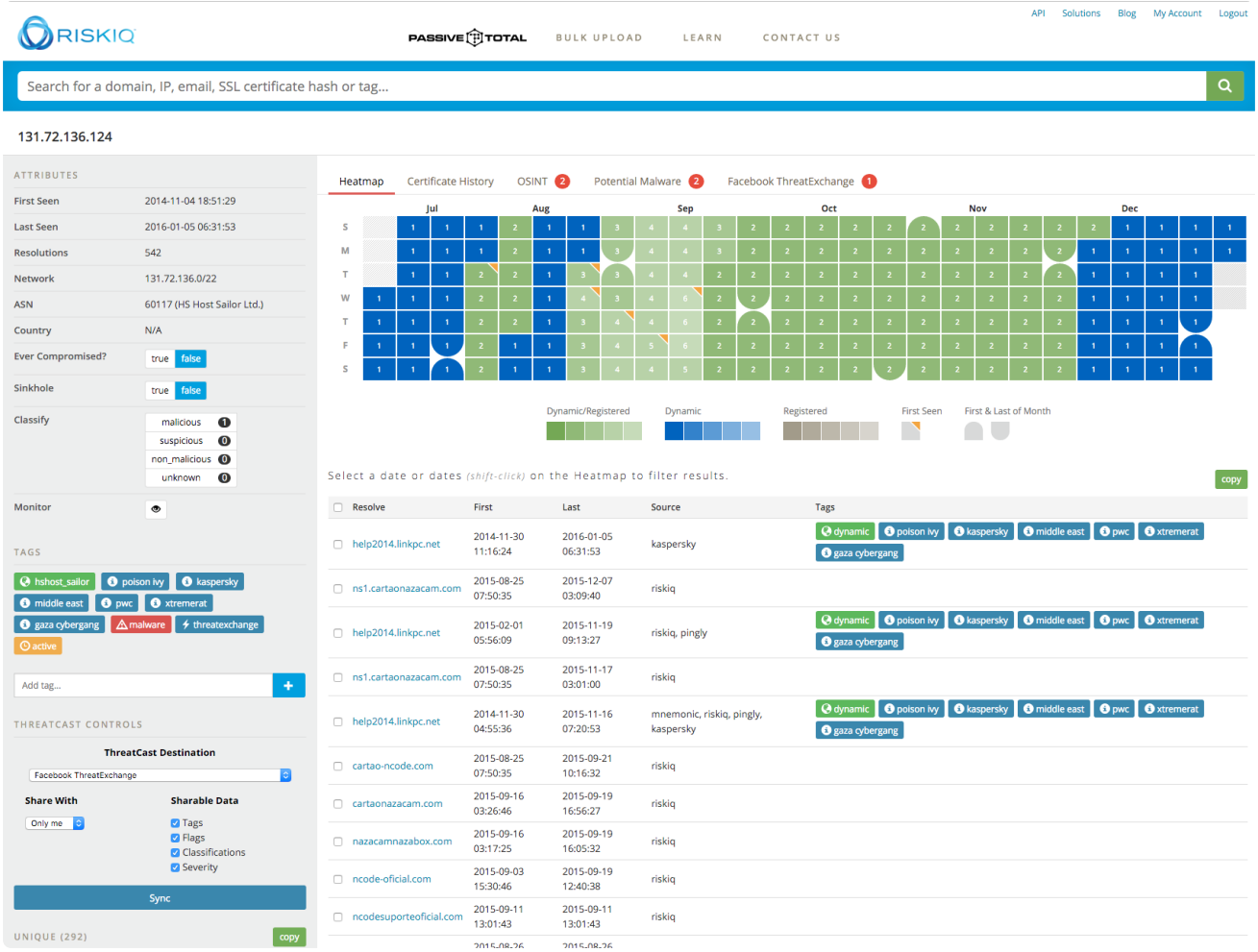
Collected	
Issued	Oct 12 11:57:52 2015 GMT
Expires	Oct 11 11:57:52 2016 GMT
Serial Number	10752693916709292470
SSL Version	2
SHA-1	e781fb12d6104c9a112c2306c1c675b47a13c8d

Common Name	www.can-i-write-any-thing.com (subject,issuer)
Organization Name	
Organization Unit	
Street Address	Oregon (subject,issuer)
Locality	Portland (subject,issuer)
State/Province	Oregon (issuer,subject)
Country	US (issuer,subject)
Serial Number	

While not incredibly unique, the common name of the certificate is interesting. Looking for open source data doesn't reveal any connections to malware, but the domain itself is strange and a good point to pivot off of.

SHA-1	First	Last	IP Addresses
2b88c745acaca4865991a65f2707191c3de726cc	2014-12-15	2015-04-13	131.72.136.132
2da15d02d83321c01454795921c5dfcb7044c96c	2014-11-24	2015-12-07	173.254.204.95
f50bbce4ba22f072b090ac018495e02459ab653d	2015-03-09	2015-03-09	46.28.203.23
9963fac3bb508273be691e08e37a551ea1d28a73	2015-10-05	2015-12-21	107.191.47.42
c43fc89f5089f7c0ea57a44474374ac8ec4041d3	2015-10-05	2015-12-07	45.32.233.125
65670d8825c79166c32e8b55a9bc551a89b7373f	2014-12-22	2015-03-16	104.131.9.135
4e989fd338b9a15cefedcf3ce47c7a703fad6a03	2014-11-24	2015-08-10	131.72.136.124
9590abb2d1b166ac209b870e8ab12e17a0c2c96a	2015-03-02	2015-03-16	198.105.117.19 198.105.117.20
4dd3e133433f8bb34e12c2bd083eca1e11acbf2a	2015-08-17	2015-12-21	104.238.162.148
e1dfbc624dc21660ce44cdb7d8df35c91b38cf43	2015-09-21	2015-11-23	108.61.198.214
b1927f7b54b5a37fdc3fbb41a7c0010b1fbe2883	2015-09-21	2015-12-21	45.32.238.65
260ba1a2835bc1c2885e730ddf0119ebd16ceca4	2015-10-12	2015-12-21	108.61.167.10
c89f069697d83c533340fcdc773493e90282bdcc	2015-10-05	2015-12-21	45.32.239.9
e32d5e93a33de29bbbb5802b2f46a939df2d795a	2015-12-14	2015-12-21	45.63.97.44
1f33a1290f5c54a0d0f02b15f23a6f4ac3b08217	2015-03-09	2015-08-24	131.72.138.229

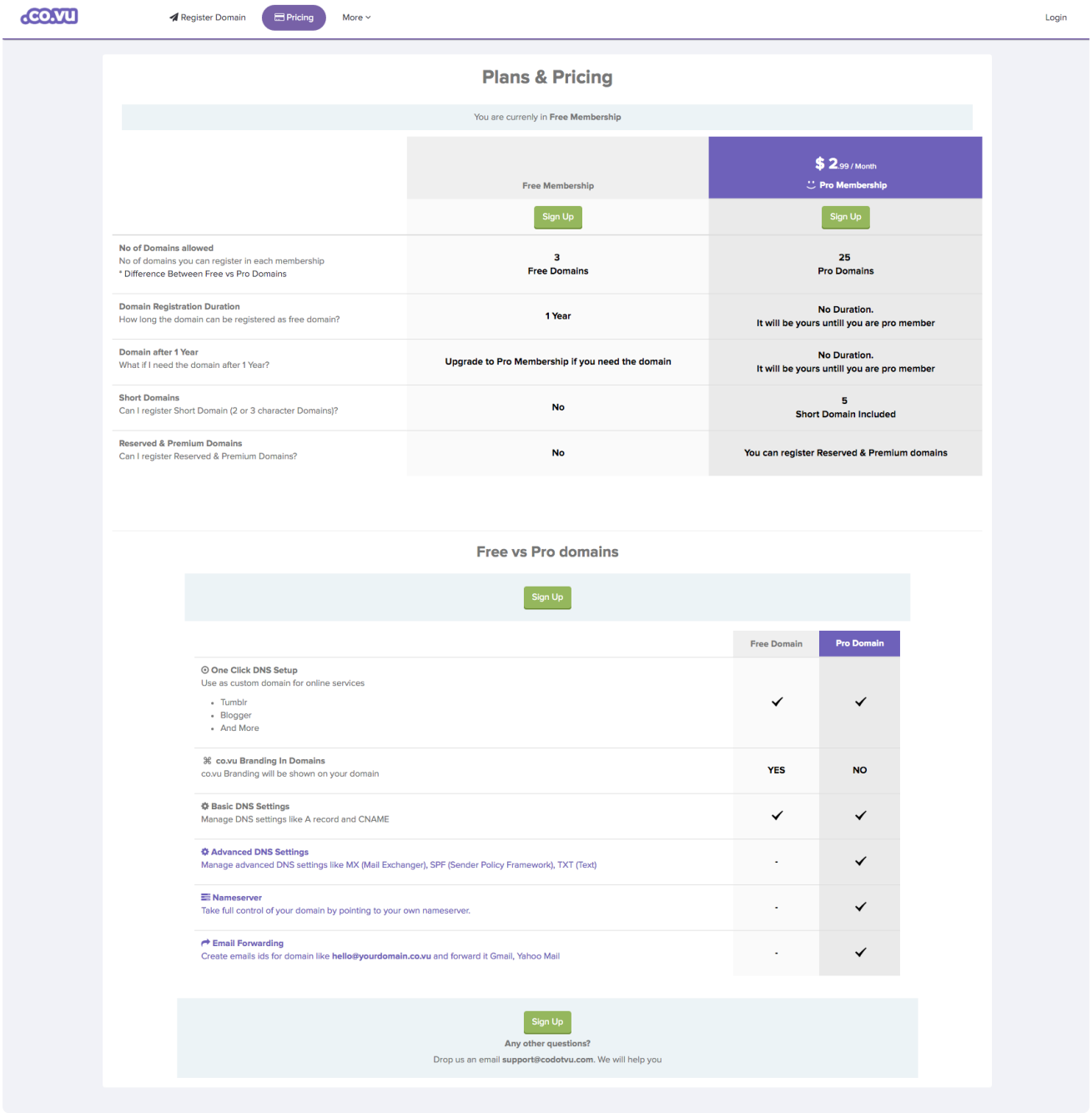
Clicking the subject name reveals quite a lot of other IP addresses that used a certificate with the same name roughly around the same 6 month time period in 2015. Many of these appear to be dead-ends, but 131.72.136.124 shows some domains associated with it that have OSINT hits associating back to PWC reporting on Middle Eastern actors using xtremeRAT and Poison Ivy and Kaspersky Gaza Cybergang.



The above results for 131.72.136.124 show yet again, an interesting change of dynamic and registered domains and then going to dynamic only in the past few weeks. Unlikely a correlation, but interesting nonetheless. The OSINT data is clearly seen by the tags on within the result table.

Co.vu

It's valuable to dig into the co.vu usage a bit more for these actors. Going to the services website reveals a dynamic-like service in which users can obfuscate their Tumblr or Blogger blog using a co.vu address.



Registering for free gives users 3 free domains they can use. Given these co.vu addresses are being used in attacks, it's worth identifying the importance of the domains. Are they being used for command and control or phishing landing pages or exploit delivery? The obfuscation on top of an already 3rd-party service shows signs that attackers are looking to hide their tracks or complicate analysis.

Share this post

Tags

research clearsky