

Operation DustySky

Clearsky
clearskysec.com/dustysky

TLP:White
For public distribution

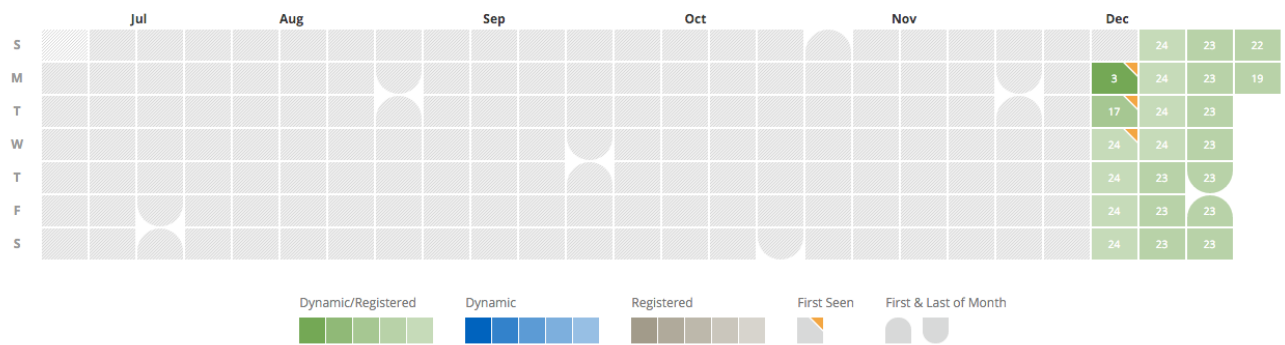


Operation DustySky Notes

Earlier this morning, Eyal from Clearsky Cyber Security published a [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.



Search for a domain, IP, email, SSL certificate hash or tag...

72.11.148.147

ATTRIBUTES

First Seen: 2012-10-07 03:43:55

Last Seen: 2016-01-04 13:52:53

Resolutions: 1932

Network: 72.11.128.0/19

ASN: 8100 (IPTTELLIGENT - IPTelligent LLC)

Country: US

Ever Compromised? true false

Sinkhole true false

Classify:
 malicious
 suspicious
 non-malicious
 unknown

Monitor

TAGS:
 iptelligent
 active

Add tag--

UNIQUE (41)

- ed3qy5joryitotursuiu.otzo.com 133
- down.downloadcor.xyz 130
- hostgatr.mrface.com 120
- down.supportcom.xyz 88
- bulk-smtp.xyz 88
- gamesonline.web.id 86
- wallnet.zyns.com 84
- ns2.indowebiz.co.id 81
- version.downloadcor.xyz 80
- gabro.xxuz.com 80

Heatmap Certificate

Collected	
Issued	Nov 25 00:00:00 2015 GMT
Expires	Nov 24 23:59:59 2016 GMT
Serial Number	71639281903408295834297330780809068825
SSL Version	2
SHA-1	8753b5eab5c3a09b4e0851c9bbd5e5036d6e9ad

Common Name	bulk-smtp.xyz (subject), COMODO RSA Domain Validation Secure Server CA (issuer)
Organization Name	COMODO CA Limited (issuer)
Organization Unit	Domain Control Validated (subject)
Street Address	Greater Manchester (issuer)
Locality	Salford (issuer)
State/Province	Greater Manchester (issuer),
Country	GB (issuer),
Serial Number	

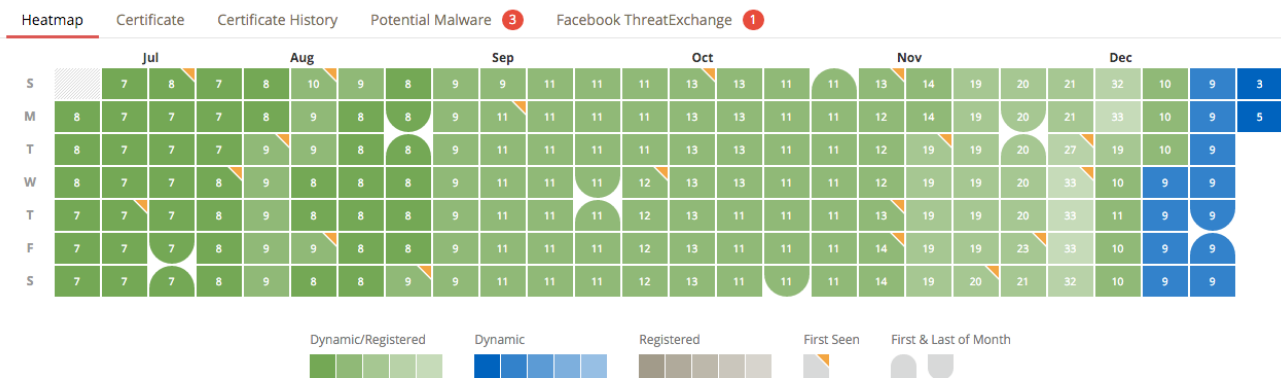
Select a date or dates (shift-click) on the Heatmap to filter results.

<input type="checkbox"/>	Resolve	First	Last	Source	Tags
<input type="checkbox"/>	bulk-smtp.xyz	2016-01-04 13:52:53	2016-01-04 13:52:53	pingly	
<input type="checkbox"/>	baz.downloadcor.xyz	2016-01-01 18:16:11	2016-01-04 12:16:14	ntotal	
<input type="checkbox"/>	info.dynamic-dns.net	2015-12-14 18:14:56	2016-01-04 12:15:58	dnsres	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	bulk-smtp.xyz	2016-01-04 10:03:38	2016-01-04 10:03:38	pingly	
<input type="checkbox"/>	baz.downloadcor.xyz	2016-01-04 04:54:55	2016-01-04 09:37:01	pingly	
<input type="checkbox"/>	wallnet.zyns.com	2016-01-04 04:54:52	2016-01-04 04:54:52	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	ed3qy5joryitotursuiu.otzo.com	2016-01-04 04:54:48	2016-01-04 04:54:48	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	krowd.downloadcor.xyz	2016-01-04 04:54:47	2016-01-04 04:54:47	pingly	
<input type="checkbox"/>	newdowr.otzo.com	2016-01-04 04:54:42	2016-01-04 04:54:42	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	direct.otzo.com	2016-01-04 04:54:40	2016-01-04 04:54:40	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	down.downloadcor.xyz	2016-01-04 04:54:31	2016-01-04 04:54:31	pingly	
<input type="checkbox"/>	vbdodo.mefound.com	2016-01-04 04:53:56	2016-01-04 04:53:56	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	supports.mefound.com	2016-01-04 04:53:53	2016-01-04 04:53:53	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	spynews.otzo.com	2016-01-04 04:53:48	2016-01-04 04:53:48	pingly	<input checked="" type="checkbox"/> dynamic
<input type="checkbox"/>	markit.mefound.com	2016-01-04 04:53:44	2016-01-04 04:53:44	pingly	<input checked="" type="checkbox"/> dynamic

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?

<input type="checkbox"/> Resolve	Location	Network	First	Last	Source	Tags
<input type="checkbox"/> 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	
<input type="checkbox"/> 192.161.48.59	US	192.161.48.0/20	2015-04-30 00:14:14	2015-07-22 04:55:28	riskiq, kaspersky	
<input type="checkbox"/> 172.227.95.162	US	172.227.80.0/20	2015-04-22 05:00:39	2015-04-22 05:59:47	mnemonic, riskiq	
<input type="checkbox"/> 192.161.48.59	US	192.161.48.0/20	2015-04-22 00:00:00	2015-04-22 00:00:00	virustotal	

Above is a screenshot of the results table from update.cisconfreak.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.

Search for a domain, IP, email, SSL certificate hash or tag...

172.227.95.162

ATTRIBUTES

First Seen 2014-11-13 21:44:01

Last Seen 2016-01-06 12:13:08

Resolutions 260

Network 172.227.80.0/20

ASN 16625 (AKAMAI-AS - Akamai Technologies)

Country US

Ever Compromised? true false

Sinkhole true false

Classify
 malicious
 suspicious
 non-malicious
 unknown

Monitor

TAGS

akamai-asn1 akamai_international_bv
 akamai_technologies middle east kaspersky
 gaza cybergang active

Add tag... +

THREATCAST CONTROLS

ThreatCast Destination

Facebook ThreatExchange

Share With Only me

Sharable Data
 Tags
 Flags
 Classifications
 Severity

Sync

UNIQUE (30)

tvnew.otzo.com	34
dancee.crabdance.com	26
testcom.strangled.net	24
tty.mooco.com	15
spreng.vizvaz.com	15
natco4.no-ip.net	14
updatee.hopto.org	14
test.cable-modem.org	12
update.mooco.com	10
www.spreng.vizvaz.com	10

1 of 3

Heatmap OSINT Certificate History Certificate

Select a date or dates (shift-click) on the Heatmap to filter results.

Resolve	First	Last	Source	Tags
<input type="checkbox"/> tvnew.otzo.com	2015-11-25 15:12:43	2016-01-06 12:13:08	dnsres	dynamic targeted middle east kaspersky gaza cybergang
<input type="checkbox"/> dancee.crabdance.com	2015-10-21 20:16:37	2016-01-06 12:13:08	dnsres	dynamic
<input type="checkbox"/> tvnew.otzo.com	2015-11-25 15:12:43	2016-01-05 21:13:34	dnsres	dynamic targeted middle east kaspersky gaza cybergang
<input type="checkbox"/> dancee.crabdance.com	2015-10-21 20:16:37	2016-01-05 21:13:34	dnsres	dynamic
<input type="checkbox"/> update.mooco.com	2015-08-25 09:26:13	2016-01-05 06:40:42	kaspersky	dynamic
<input type="checkbox"/> tvnew.otzo.com	2015-02-20 05:57:20	2016-01-05 06:40:27	kaspersky	dynamic targeted middle east kaspersky gaza cybergang
<input type="checkbox"/> tty.mooco.com	2015-03-29 01:03:47	2016-01-05 06:40:19	kaspersky	dynamic
<input type="checkbox"/> testcom.strangled.net	2015-03-26 04:59:31	2016-01-05 06:39:51	kaspersky	dynamic middle east kaspersky gaza cybergang
<input type="checkbox"/> dancee.crabdance.com	2015-02-20 05:57:25	2016-01-05 06:29:00	kaspersky	dynamic
<input type="checkbox"/> ahw.wha.la	2015-12-15 00:54:46	2016-01-05 06:26:24	kaspersky	dynamic
<input type="checkbox"/> update.mooco.com	2015-08-25 09:26:13	2016-01-04 06:50:48	kaspersky	dynamic
<input type="checkbox"/> tty.mooco.com	2015-03-29 01:03:47	2016-01-04 06:50:24	kaspersky	dynamic
<input type="checkbox"/> tvnew.otzo.com	2015-02-20 05:57:20	2016-01-04 06:50:22	kaspersky	dynamic targeted middle east kaspersky gaza cybergang
<input type="checkbox"/> testcom.strangled.net	2015-03-26 04:59:31	2016-01-04 06:49:44	kaspersky	dynamic middle east kaspersky gaza cybergang
<input type="checkbox"/> dancee.crabdance.com	2015-02-20 05:57:25	2016-01-04 06:36:26	kaspersky	dynamic

malicious suspicious non-malicious unknown add tag... +

1 2 3 4 5

1 of 18

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	<u>Certificate</u>
---------	---------------------	--------------------

Collected		Common Name	www.can-i-write-any-thing.com (subject,issuer)
Issued	Oct 12 11:57:52 2015 GMT	Organization Name	
Expires	Oct 11 11:57:52 2016 GMT	Organization Unit	
Serial Number	10752693916709292470	Street Address	Oregon (subject,issuer)
SSL Version	2	Locality	Portland (subject,issuer)
SHA-1	e781fb12d6104c9a112c2306c1c675b47a13c8d	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.

<input type="checkbox"/>	SHA-1	First	Last	IP Addresses
<input type="checkbox"/>	2b88c745acaca4865991a65f2707191c3de726cc	2014-12-15	2015-04-13	131.72.136.132
<input type="checkbox"/>	2da15d02d83321c01454795921c5dfcb7044c96c	2014-11-24	2015-12-07	173.254.204.95
<input type="checkbox"/>	f50bbce4ba22f072b090ac018495e02459ab653d	2015-03-09	2015-03-09	46.28.203.23
<input type="checkbox"/>	9963fac3bb508273be691e08e37a551ea1d28a73	2015-10-05	2015-12-21	107.191.47.42
<input type="checkbox"/>	c43fc89f50897c0ea57a44474374ac8ec4041d3	2015-10-05	2015-12-07	45.32.233.125
<input type="checkbox"/>	65670d8825c79166c32e8b55a9bc551a89b7373f	2014-12-22	2015-03-16	104.131.9.135
<input type="checkbox"/>	4e989fd338b9a15cefedcf3ce47c7a703fad6a03	2014-11-24	2015-08-10	131.72.136.124
<input type="checkbox"/>	9590abb2d1b166ac209b870e8ab12e17a0c2c96a	2015-03-02	2015-03-16	198.105.117.19 198.105.117.20
<input type="checkbox"/>	4dd3e133433f8bb34e12c2bd083eca1e11acbf2a	2015-08-17	2015-12-21	104.238.162.148
<input type="checkbox"/>	e1dfbc624dc21660ce44cdb7d8df35c91b38cf43	2015-09-21	2015-11-23	108.61.198.214
<input type="checkbox"/>	b1927f7b54b5a37fdc3fbb41a7c0010b1fbc2883	2015-09-21	2015-12-21	45.32.238.65
<input type="checkbox"/>	260ba1a2835bc1c2885e730ddf0119ebd16ceca4	2015-10-12	2015-12-21	108.61.167.10
<input type="checkbox"/>	c89f069697d83c533340fcdc773493e90282bdcc	2015-10-05	2015-12-21	45.32.239.9
<input type="checkbox"/>	e32d5e93a33de29bbbb5802b2f46a939df2d795a	2015-12-14	2015-12-21	45.63.97.44
<input type="checkbox"/>	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.

Search for a domain, IP, email, SSL certificate hash or tag...

131.72.136.124

ATTRIBUTES

First Seen: 2014-11-04 18:51:29
 Last Seen: 2016-01-05 06:31:53
 Resolutions: 542
 Network: 131.72.136.0/22
 ASN: 60117 (HS Host Sailor Ltd.)
 Country: N/A
 Ever Compromised?: true false
 Sinkhole: true false

Classify

- malicious
- suspicious
- non_malicious
- unknown

Monitor

TAGS

hshost_sailor, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang, malware, threatexchange, active

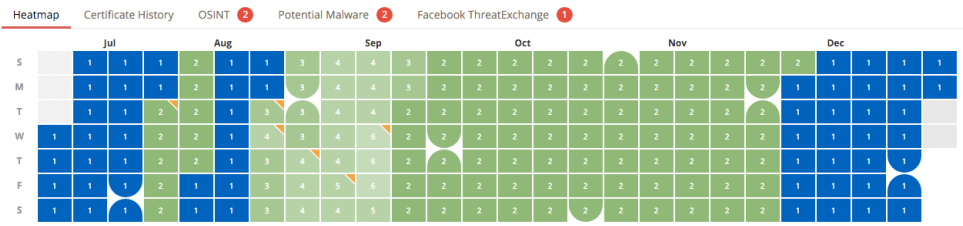
THREATCAST CONTROLS

ThreatCast Destination: Facebook ThreatExchange

Share With: Only me

Sharable Data: Tags, Flags, Classifications, Severity

UNIQUE (292)



Select a date or dates (shift-click) on the Heatmap to filter results.

<input type="checkbox"/> Resolve	First	Last	Source	Tags
<input type="checkbox"/>	help2014.linkpc.net 2014-11-30 11:16:24	2016-01-05 06:31:53	kaspersky	dynamic, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang
<input type="checkbox"/>	ns1.cartanazacam.com 2015-08-25 07:50:35	2015-12-07 03:09:40	riskiq	dynamic, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang
<input type="checkbox"/>	help2014.linkpc.net 2015-02-01 05:56:09	2015-11-19 09:13:27	riskiq, pingly	dynamic, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang
<input type="checkbox"/>	ns1.cartanazacam.com 2015-08-25 07:50:35	2015-11-17 03:01:00	riskiq	dynamic, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang
<input type="checkbox"/>	help2014.linkpc.net 2014-11-30 04:55:36	2015-11-16 07:20:53	mnemonic, riskiq, pingly, kaspersky	dynamic, poison Ivy, kaspersky, middle east, pwc, xtrememat, gaza cybergang
<input type="checkbox"/>	cartao-ncode.com 2015-08-25 07:50:35	2015-09-21 10:16:32	riskiq	
<input type="checkbox"/>	cartanazacam.com 2015-09-16 03:26:46	2015-09-19 16:56:27	riskiq	
<input type="checkbox"/>	nazacamnazabox.com 2015-09-16 03:17:25	2015-09-19 16:05:32	riskiq	
<input type="checkbox"/>	ncode-oficial.com 2015-09-03 15:30:46	2015-09-19 12:40:38	riskiq	
<input type="checkbox"/>	ncodesuporteoficial.com 2015-09-11 13:01:43	2015-09-11 13:01:43	riskiq	

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.

Plans & Pricing

You are currently in Free Membership

	Free Membership	\$2.99 / Month Pro Membership
	Sign Up	Sign Up
No of Domains allowed No of domains you can register in each membership * Difference Between Free vs Pro Domains	3 Free Domains	25 Pro Domains
Domain Registration Duration How long the domain can be registered as free domain?	1 Year	No Duration. It will be yours until you are pro member
Domain after 1 Year What if I need the domain after 1 Year?	Upgrade to Pro Membership if you need the domain	No Duration. It will be yours until you are pro member
Short Domains Can I register Short Domain (2 or 3 character Domains)?	No	5 Short Domain Included
Reserved & Premium Domains Can I register Reserved & Premium Domains?	No	You can register Reserved & Premium domains

Free vs Pro domains

	Free Domain	Pro Domain
One Click DNS Setup Use as custom domain for online services • Tumblr • Blogger • And More	✓	✓
co.vu Branding In Domains co.vu Branding will be shown on your domain	YES	NO
Basic DNS Settings Manage DNS settings like A record and CNAME	✓	✓
Advanced DNS Settings Manage advanced DNS settings like MX (Mail Exchanger), SPF (Sender Policy Framework), TXT (Text)	-	✓
Nameserver Take full control of your domain by pointing to your own nameserver.	-	✓
Email Forwarding Create emails ids for domain like <code>hello@yourdomain.co.vu</code> and forward it Gmail, Yahoo Mail	-	✓

[Sign Up](#)

Any other questions?

Drop us an email support@codotvu.com. We will help you

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