swannysec

Uncovering a New Angler-Bedep Actor

12 Apr 2016

Tags: Analysis, Angler, Bedep

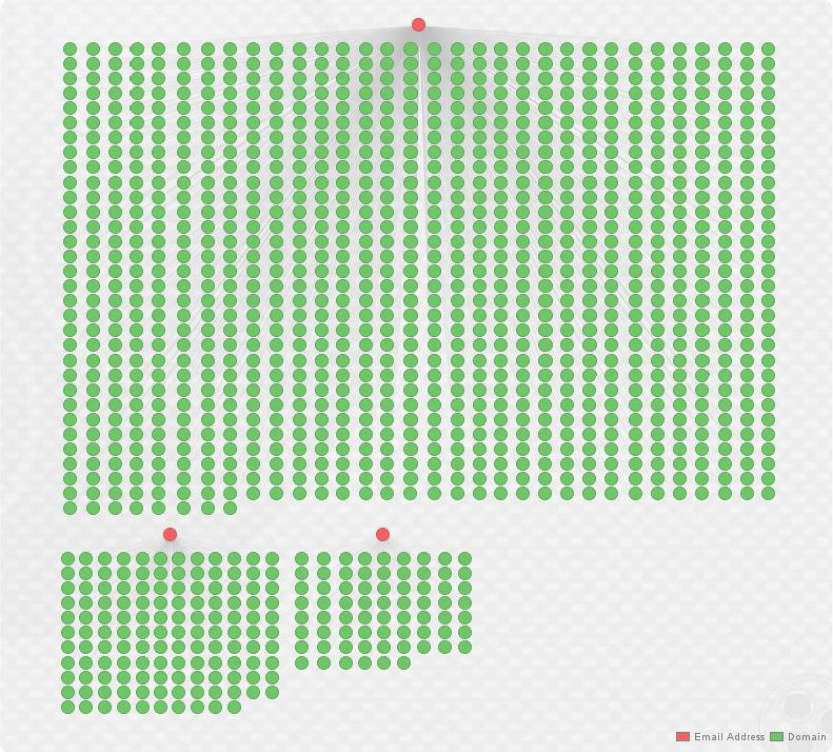
Some time ago, I did some analysis that linked a fairly run-of-the-mill Torrentlocker distribution network to actors and infrastructure delivering Pony. I promised some follow-up on that, and it's still coming, but it's proving to be a bit of a rabbit hole. I need some more time to dot my i's and cross my t's, but I hope to have something to share soon.

In the meantime, I wanted to take some time to write up another piece of research I recently completed on a group of well known Angler EK and Bedep actors. If you've followed along with Angler and Bedep over the last year or so, you'll no doubt be familiar with yingw90@yahoo.com, potrafamin44as@gmail.com, and john.bruggink@yahoo.co.uk. These accounts are responsible for the registration of large numbers of domains associated with the distribution of Angler EKs and Bedep, as well as some other unpleasant creatures such as Kazy and Symmi. For more information, check out this great write-up from Nick Biasini over at Talos. An Alienvault OTX pulse with all the goodies is available, likely from Alex Pinto at Niddel, here.

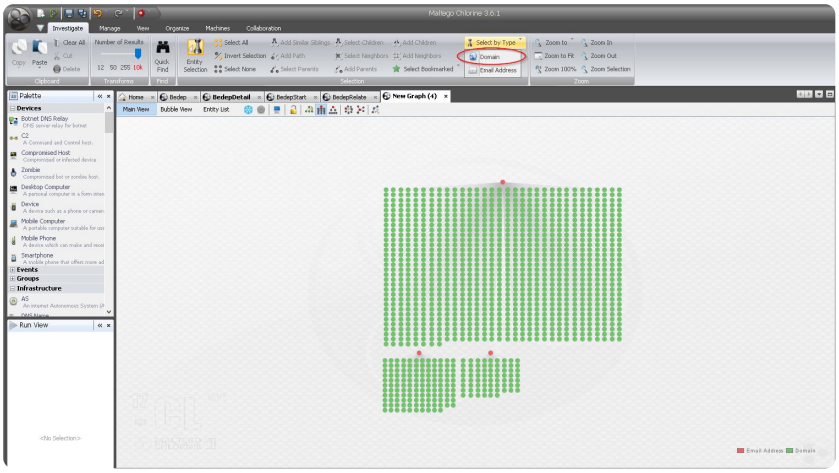
Now that you're familiar with the campaign in question, let's take a deep-dive. For this analyis, I will be using Paterva's Maltego loaded with transforms from two fantastic sources, PassiveTotal and ThreatCrowd. These are fantastic tools with free options that can get you started on some great analysis, so give them a try!

To begin, I entered the three well-known actors referenced above as e-mail entities in Maltego:

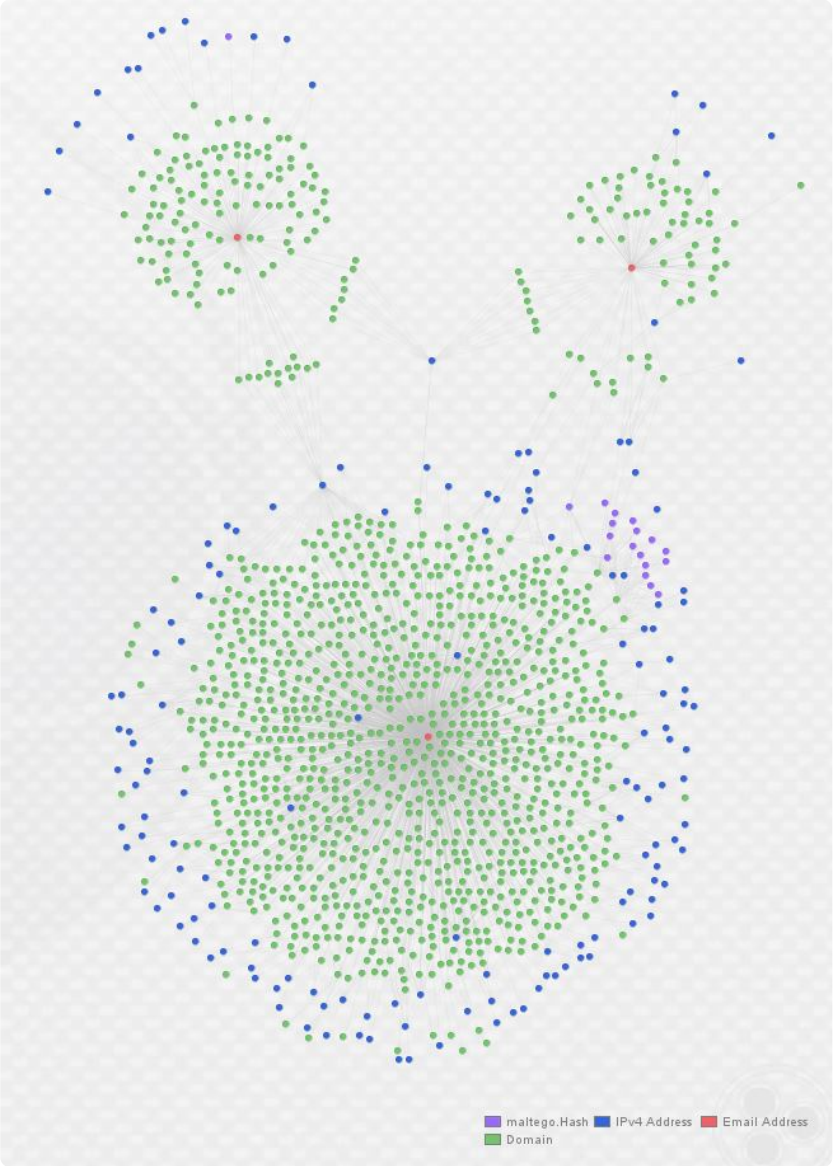
Once entered, I started by utilizing PassiveTotal to return all known domains registered by these addresses as shown in the screenshot below (do note that you could manually import these from the Alienvault IOCs provided above, as well). The results follow in the second image, that's a lot of domains!



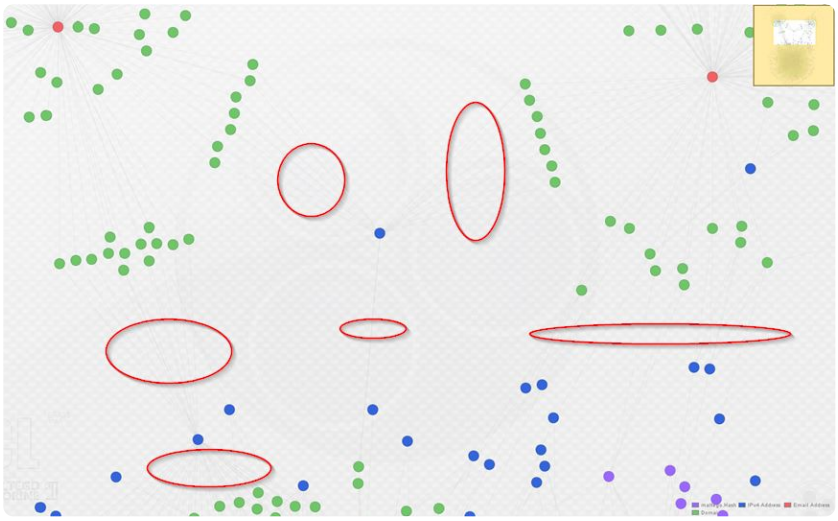
Enter ThreatCrowd. Let's go ahead and enrich each of these domains with any available information ThreatCrowd has to offer (sorry for the API load, Chris!). Select all the domains as follows:



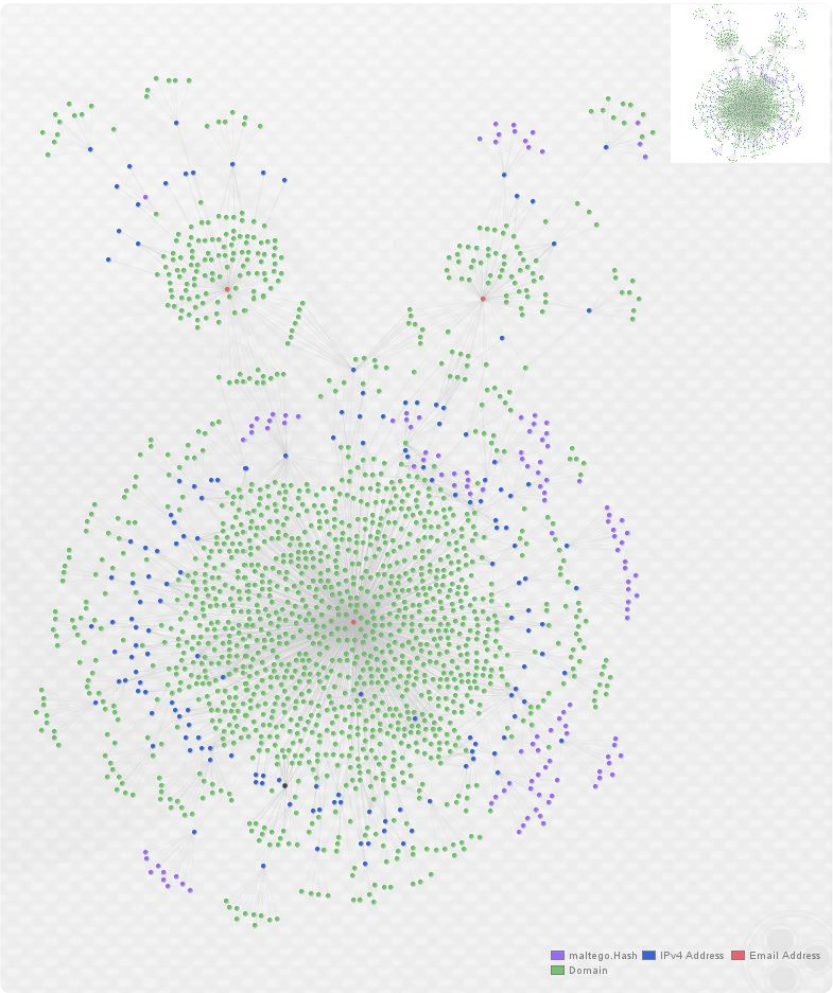
Once you have all the domains selected, use the following transform from ThreatCrowd. The results are below.



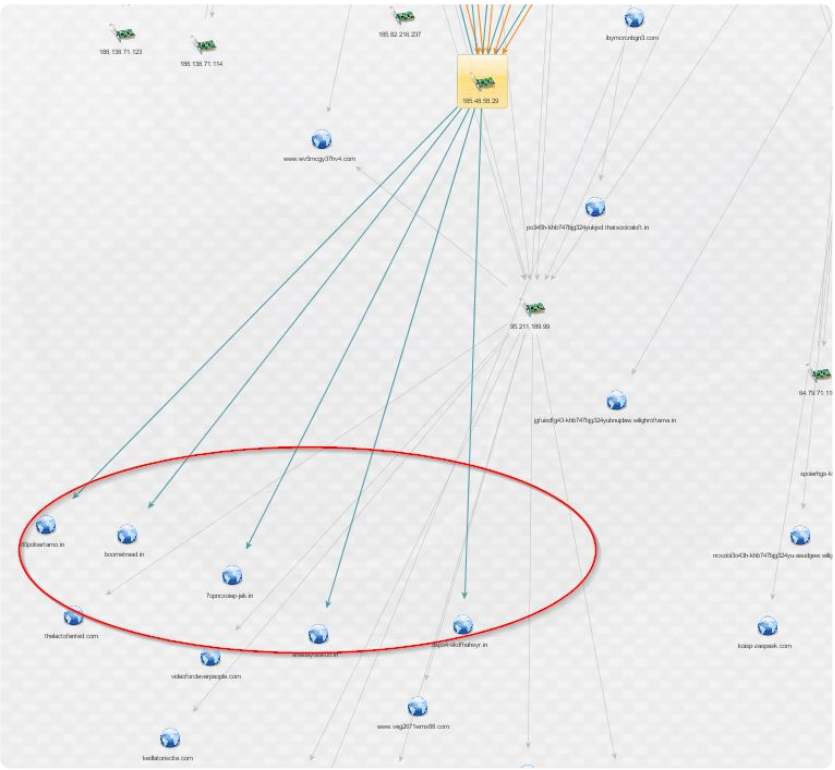
As you can see above, I've re-arranged the graph into the Organic layout in order to make the clustering around each registrant e-mail (in red) apparent. Below, observe a zoomed view of the links indicating domains from each cluster sharing IP infrastructure. The links are hard to see, so I circled them in red:



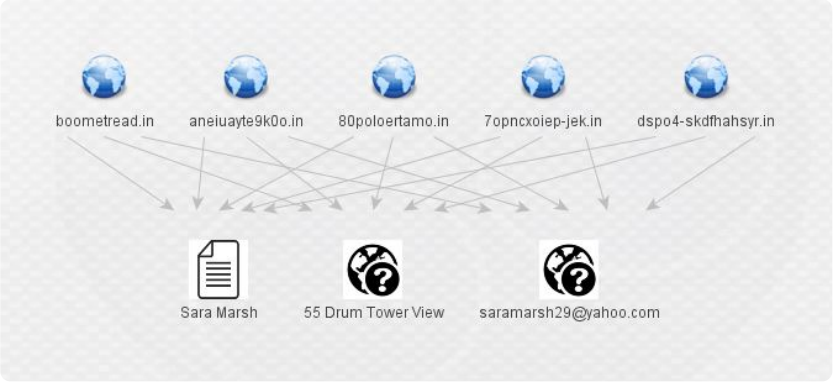
At this point, we have clear overlap between these three actors as they're utilizing some of the same hosting providers and individual hosts to serve malicious domains. In order to go one step further, I expanded the graph again, this time by enriching all IP addresses with ThreatCrowd. (A note of caution here: this can return large number of domains if an IP you choose to expand is a large webhost, so take care to double-check whether returned entities are relevant.) Here's what the graph looks like after one round of domain enrichment and one round of IP enrichment:



From here, I began working through new clusters of domains looking for new leads by checking whois records with PassiveTotal and looking for malware and other associated infrastructure with ThreatCrowd. After hunting around for a while, I discovered the following indicator, with new domains discovered from it circled in red:



This indicator uncovered something new. Below is a fresh graph, for clarity, containing the new domains discovered from that IP, followed by their enrichment via PassiveTotal's whois details (scrubbed of all but registrant name, e-mail, and address):



Who is Sara Marsh, why is she registering obviously junky (and potentially DGA-generated) domains, and why is she

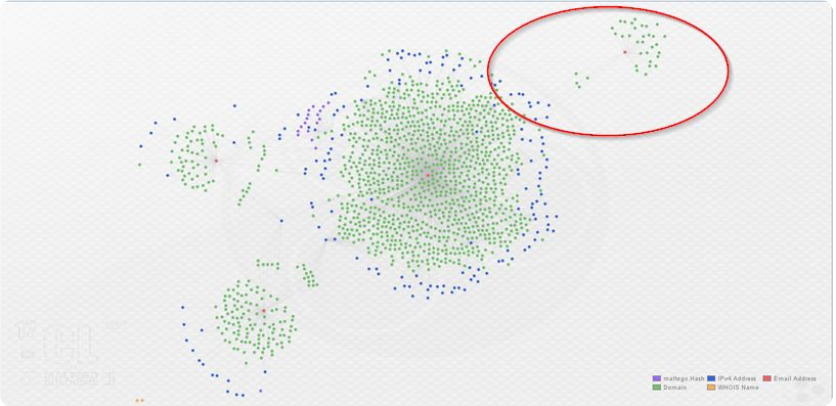
sharing infrastructure with the likes of the actors we started with? At this point, I almost hit a dead end. Most of my normal, publicly available sources had no information of significance on Sara Marsh, her e-mails, or the domains she registered. ThreatCrowd showed her domains as adjacent to, but not directly hosting malware. Alienvault OTX had no information on her or her domains, and neither did most of the other sources I usually check. However, good old-fashioned google came to the rescue. A quick search of the new e-mail address revealed a pastebin paste from an anonymous source that referenced saramarsh29@yahoo.com.


```
Post-compromise Bedep traffic observed to destina
tion domains bokoretanom()net, op23jhsoaspo()in,
 koewasoul()com, and dertasolope7com()com.

Observed referers (forged - machines never actual
ly browsed to the referers):  loervites()com, new
blackfridayads()com, alkalinerooms()net, new-apri
l-discount()net, violatantati()com, nicedicecools
()net, books-origins-dooms()net, adsforbussiness-
new()com

Observed traffic patterns:
/ads.php?sid=1923
/advertising.html
/ads.js
/media/ads.js
/r.php?key=a5ec17eed153654469be424b96891e79

Summary:
Bedep immediately opens a backdoor on the target
 machine; it also generates click-fraud traffic,
 and can be used to load further malware.  Bedep
 was written by the authors of the Angler Exploit
Kit, and as such, AnglerEK is the primary distrib
ution method for this malware.

All observed domains are registered to Sara Marsh
(saramarsh29@yahoo.com) and Gennadiy Borisov (yin
gw90@yahoo.com) through Domain Context.  These ar
e certainly fake names and email addresses, but a
ppear to be used often.  As such, they are reliab
```

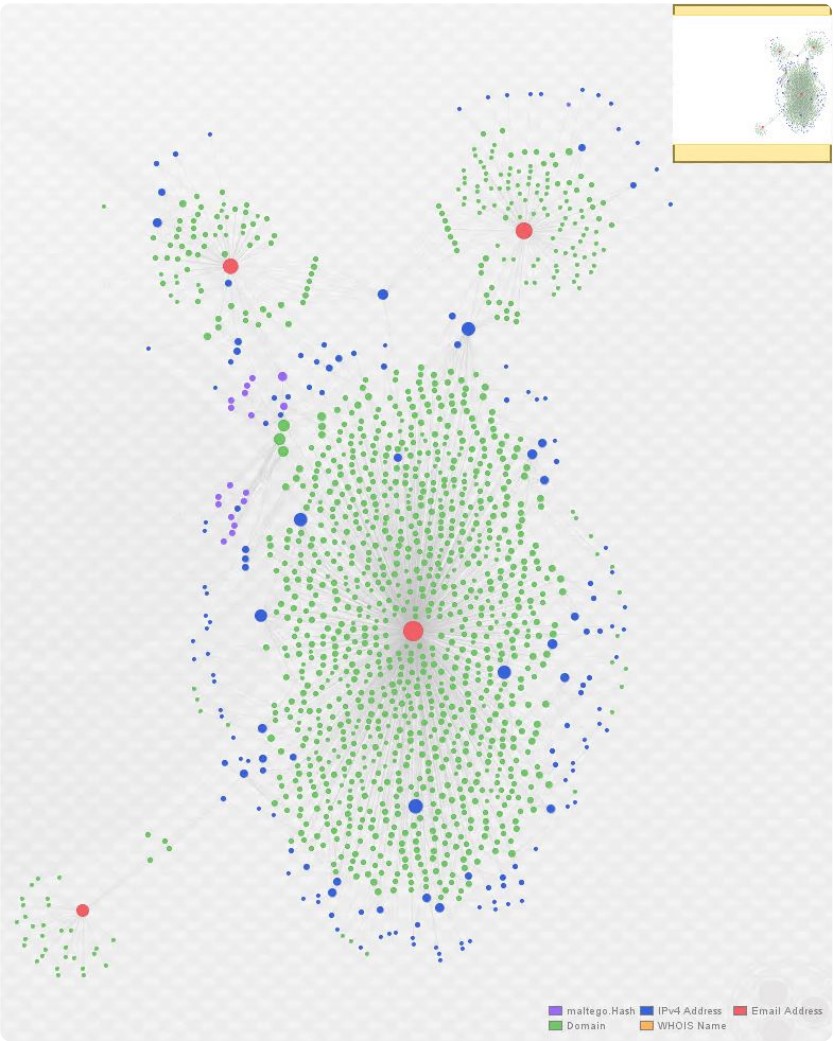
```
le indicators, for the time being, that a domain
 is malicious.
```

While I don't usually rely on anonymous sources, this simply served to confirm what was already fairly apparent from appearances. This was backed up by the presence of saramarsh29@yahoo.com on malekal.com's malwaredb, sharing an IP with a domain from none other than potrafamin44as@gmail.com.

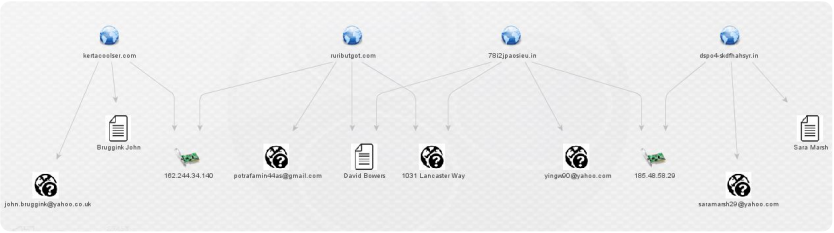
At this stage, I added saramarsh29@yahoo.com back to our original graph, and used PassiveTotal to return all domains registered to that address. The result is below:



Here's an additional representation using bubble view. This view adjusts the size of the entities based, in this case, on the number of links associated with them. Again, the actor e-mails are in red:



By now, it is readily apparent that we've uncovered an additional actor in this Angler EK/Bedep campaign. In order to further demonstrate some of the relationships between these actors, I selected four related domains from the graph above, moved them to a fresh graph, and enriched them with both ThreatCrowd and PassiveTotal (displaying only relevant results):



The above image displays in a nutshell the close relationship between these actors. Nick Biasini did some fine work in uncovering the first three actors; now a fourth is apparent as well. A list of domains registered to saramarsh29@yahoo.com is below; this can also be found

in an Alienvault OTX pulse which is embedded below. The same list and the Maltego graph are available on my GitHub repo.

As always, I appreciate any feedback; give me a shout @swannysec.

Likely Angler EK/Bedep Domains Registered by saramarsh29@yahoo.com:

```
qwmpo347xmnopw[.]in
alkalinerooms[.]net
swimming-shower[.]com
guy-doctor-eye[.]com
dertasolope7com[.]com
abronmalowporetam[.]in
j3u3poolre[.]in
joomboomrats[.]com
7opncxoiep-jek[.]in
violatantati[.]com
xvuxemuhdusxqfyt[.]com
lsaopajipwlo-sopqkmo[.]in
fl4o5i58kdbss[.]in
aneiuayte9k0o[.]in
term-spread-medicine[.]com
betterstaffprofit[.]com
ldsfo409salkopsh[.]in
bokoretanom[.]net
geraldfrousers[.]net
boometread[.]in
80poloertamo[.]in
newblackfridayads[.]com
books-origins-dooms[.]net
shareeffect-affair[.]com
loervites[.]com
axenndnyotxkohhf69[.]com
art-spite-tune[.]com
vewassorthenha[.]in
ruributgot[.]in
1000mahbatterys[.]com
xcmno54pjasghg[.]in
trusteer-tech[.]com
adsforbussiness-new[.]com
nicedicecools[.]net
xbvioep4naop[.]in
taxrain-bottom[.]com
dspo4-skdfhahsyr[.]in
```

Related Posts

On Risk, Incident Response, and Coronavirus 08 Mar 2020

Brian Krebs and the Yugoslavian Business Network - Analyzing Nebula 07 Mar 2017

Changing Things Up 09 Aug 2016

Author: John D. Swanson - Contact me at swanson.john.d@gmail.com
Opinions are my own and do not reflect those of my employer.