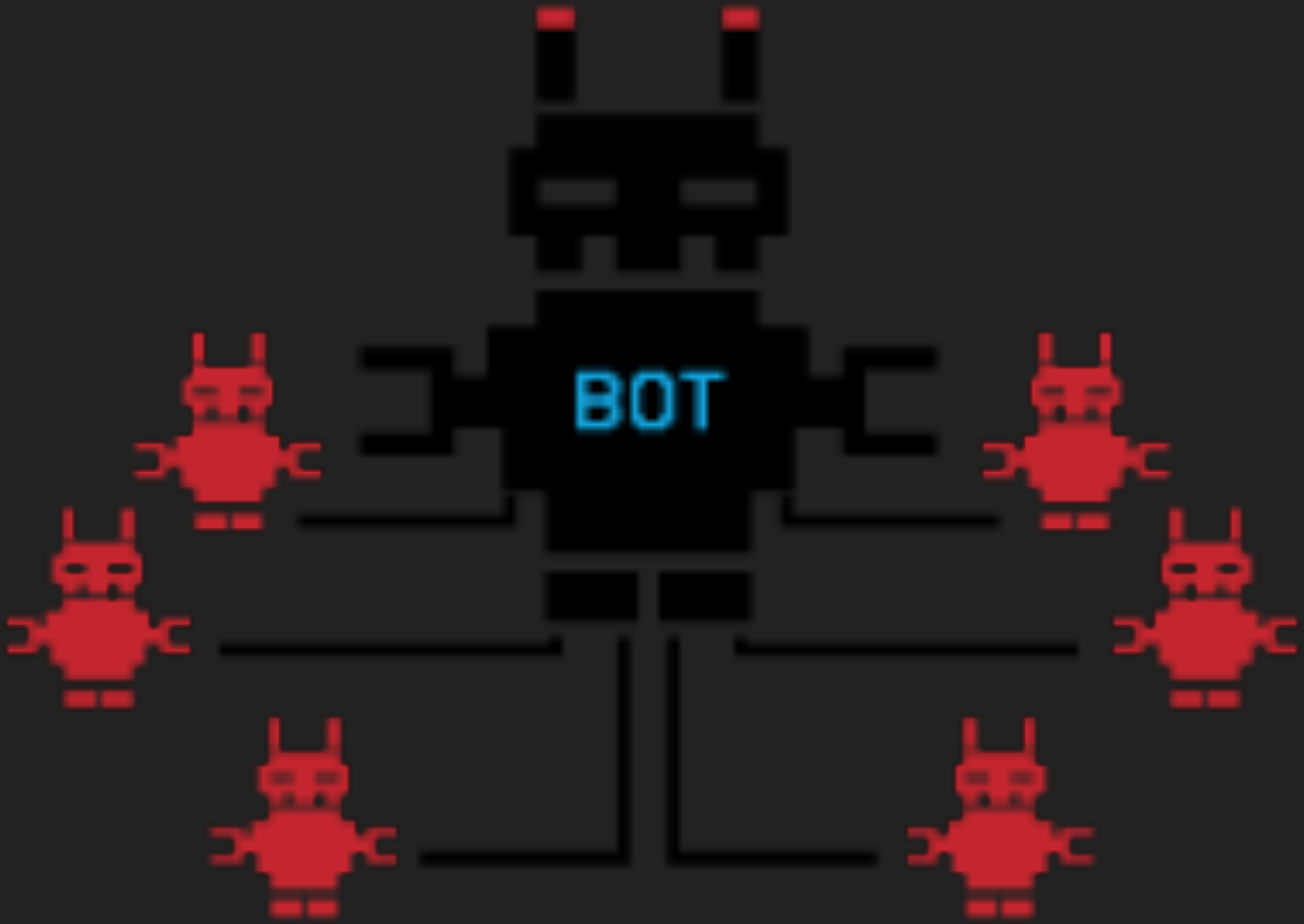


UNCOVERING AND VISUALIZING BOTNET INFRASTRUCTURE AND BEHAVIOR

DEEPSEC

ANDREA SCARFO (SECURITY RESEARCHER)

Security Research Analyst @ Cisco Umbrella (formerly OpenDNS) in San Francisco since 2015

cisco

Cisco Umbrella

OpenDNS

Previously a System Administrator for 12 years

hp

DANVILLE

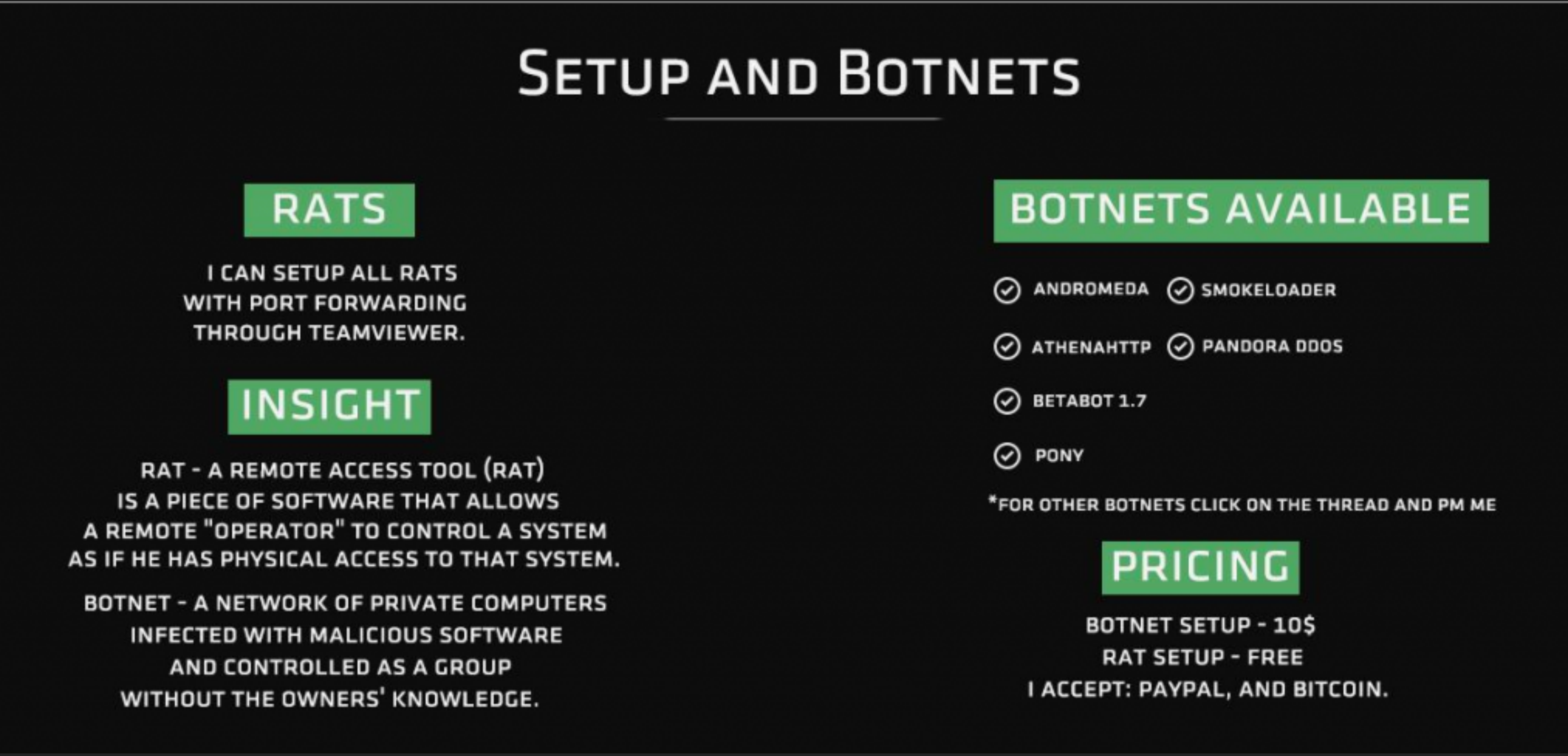
KRAFT

JOSH PYORRE (SECURITY RESEARCHER)

- Cisco Umbrella
- NASA
- Mandiant

WHAT IS A BOTNET?

Page Advertising botnet services for sale on dark web



SETUP AND BOTNETS

RATS

I CAN SETUP ALL RATS
WITH PORT FORWARDING
THROUGH TEAMVIEWER.

INSIGHT

RAT - A REMOTE ACCESS TOOL (RAT)
IS A PIECE OF SOFTWARE THAT ALLOWS
A REMOTE "OPERATOR" TO CONTROL A SYSTEM
AS IF HE HAS PHYSICAL ACCESS TO THAT SYSTEM.

BOTNET - A NETWORK OF PRIVATE COMPUTERS
INFECTED WITH MALICIOUS SOFTWARE
AND CONTROLLED AS A GROUP
WITHOUT THE OWNERS' KNOWLEDGE.

BOTNETS AVAILABLE

- ✓ ANDROMEDA
- ✓ ATHENAHTTP
- ✓ BETABOT 1.7
- ✓ PONY
- ✓ SMOKELOADER
- ✓ PANDORA DDOS

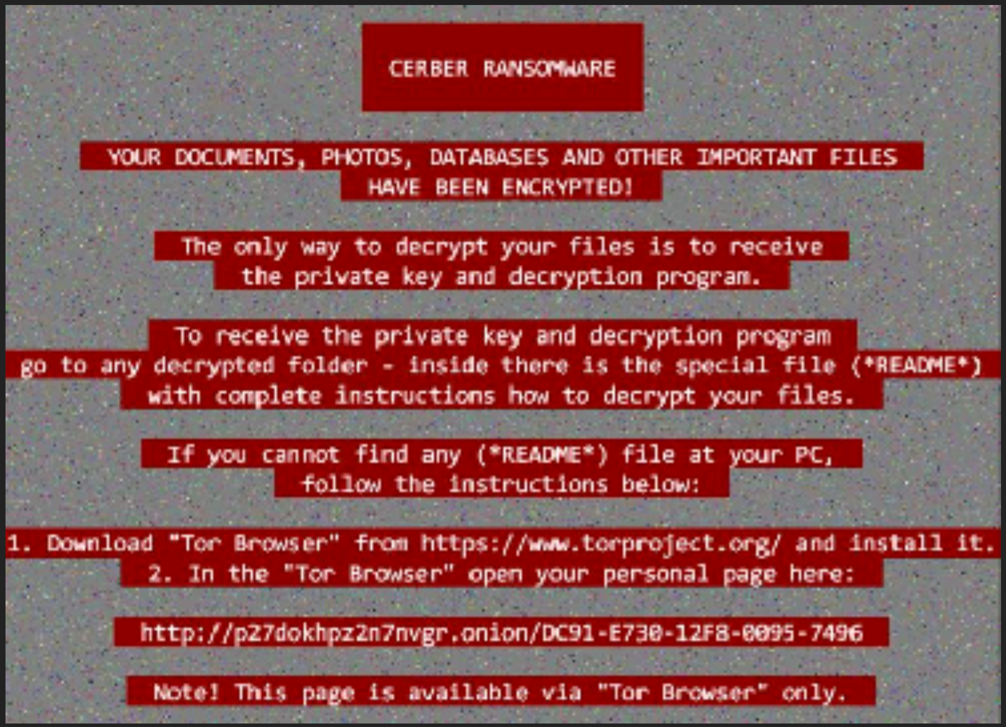
*FOR OTHER BOTNETS CLICK ON THE THREAD AND PM ME

PRICING

BOTNET SETUP - 10$
RAT SETUP - FREE
I ACCEPT: PAYPAL, AND BITCOIN.

Different uses for botnets

CRIMINAL ACTIVITY



CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive the private key and decryption program.

To receive the private key and decryption program go to any decrypted folder - inside there is the special file (*README*) with complete instructions how to decrypt your files.

If you cannot find any (*README*) file at your PC, follow the instructions below:

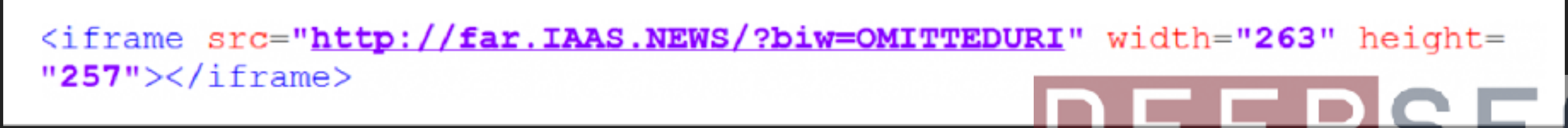
1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

http://p27dokhpz2n7nvgr.onion/DC91-E730-12F8-0095-7496

Note! This page is available via "Tor Browser" only.

Click here!!

$$$$$$$$$$$$$$



```
<iframe src="http://far.IAAS.NEWS/?biw=OMITTEDURI" width="263" height=
"257"></iframe>
```

WHY VISUALS

- Helps turn data into actionable meaningful information
- You shouldn’t block every IOC
- Able to quickly see the connections/relationships of attack campaigns with botnets

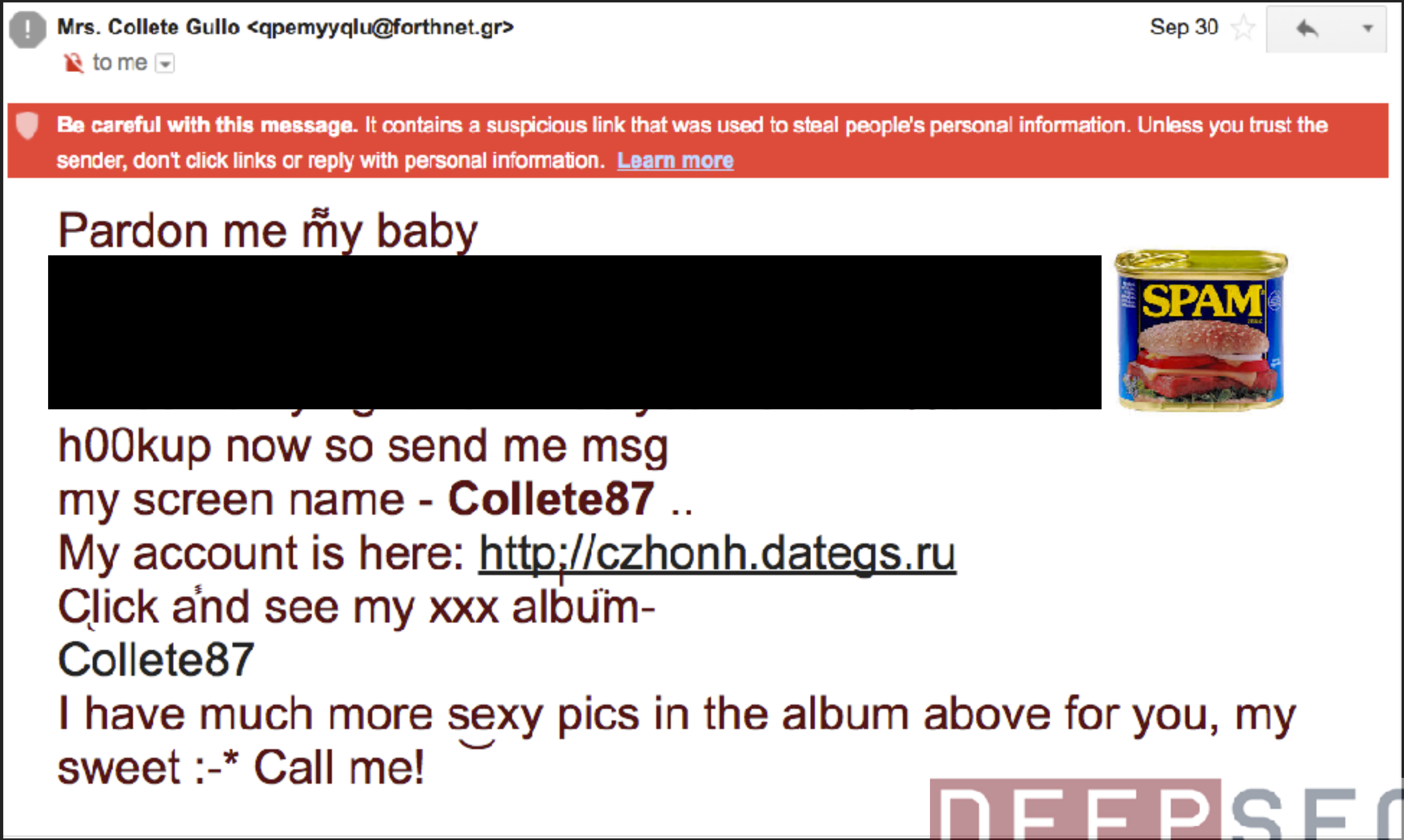
LIFECYCLE OF A BOT

INFECTION

&

SPREADING

INFECTION AND SPREADING : SPAM



Mrs. Collete Gullo <qpemyyqlu@forthnet.gr>

to me

Sep 30

Be careful with this message. It contains a suspicious link that was used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Pardon me m̃y baby

[redacted]

h00kup now so send me msg

my screen name - **Collete87** ..

My account is here: http://czhonh.dategs.ru

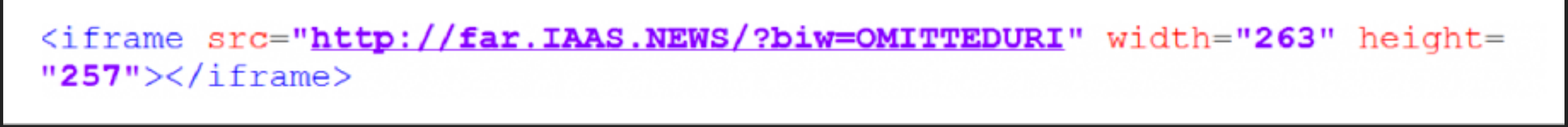
Click ańd see my xxx albüm-

Collete87

I have much more sexy pics in the album above for you, my sweet :-* Call me!

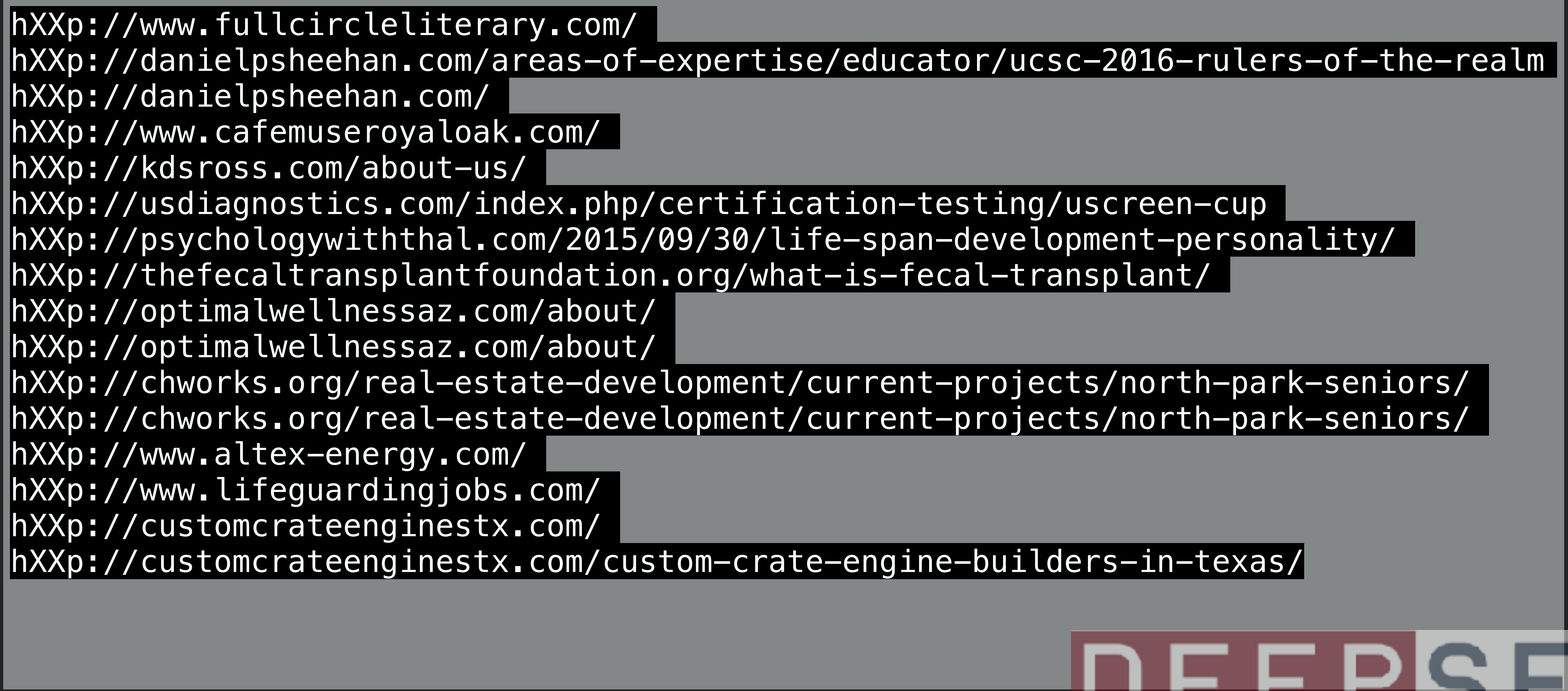
Injected iframe in compromised site

INFECTION AND SPREADING : WEBSITE COMPROMISE



```
<iframe src="http://far.IAAS.NEWS/?biw=OMITTEDURI" width="263" height=
"257"></iframe>
```

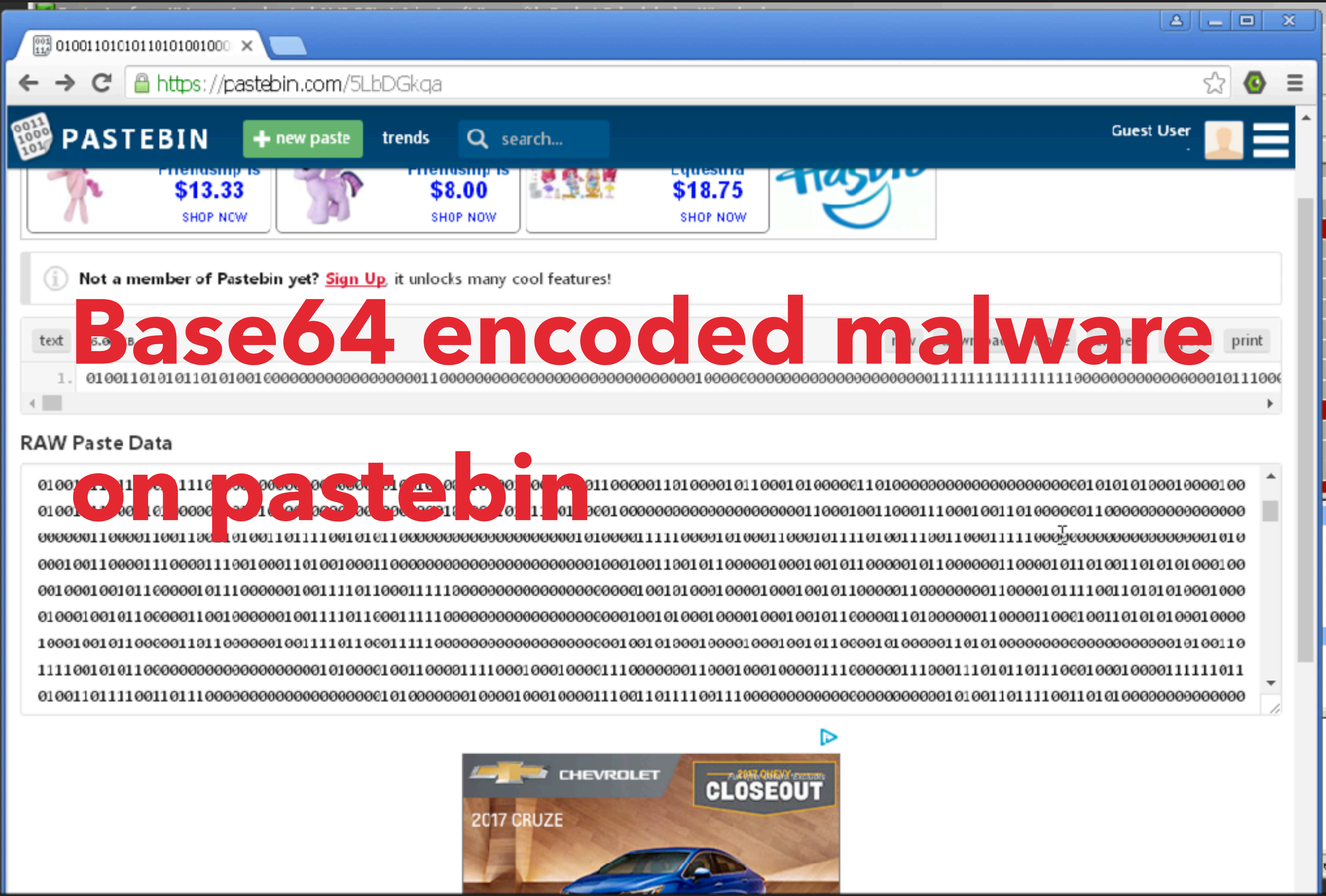
Compromised sites sending to site in iframe



```
hXXp://www.fullcircleliterary.com/
hXXp://danielpsheehan.com/areas-of-expertise/educator/ucsc-2016-rulers-of-the-realm
hXXp://danielpsheehan.com/
hXXp://www.cafemuseroyaloak.com/
hXXp://kdsross.com/about-us/
hXXp://usdiagnostics.com/index.php/certification-testing/uscreen-cup
hXXp://psychologywiththal.com/2015/09/30/life-span-development-personality/
hXXp://thefecaltransplantfoundation.org/what-is-fecal-transplant/
hXXp://optimalwellnessaz.com/about/
hXXp://optimalwellnessaz.com/about/
hXXp://chworks.org/real-estate-development/current-projects/north-park-seniors/
hXXp://chworks.org/real-estate-development/current-projects/north-park-seniors/
hXXp://www.altex-energy.com/
hXXp://www.lifeguardingjobs.com/
hXXp://customcrateenginestx.com/
hXXp://customcrateenginestx.com/custom-crate-engine-builders-in-texas/
```

INFECTION AND SPREADING : RATS

Base64 encoded malware on pastebin



Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

```
1. 0100110101011010100100000000000000000000110000000000000000000000000000000100000000000000000000000000000011111111111111100000000000000000010111000
```

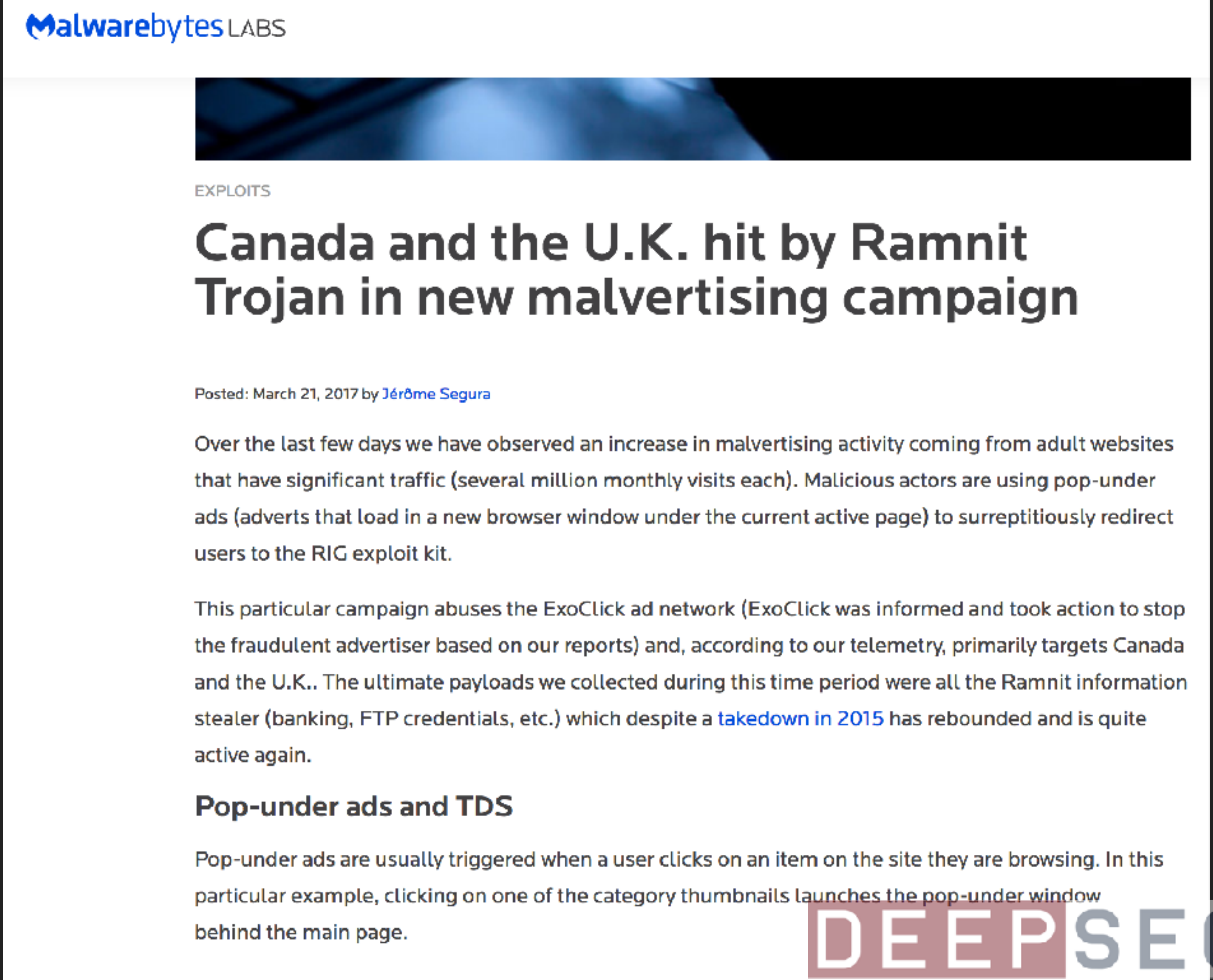
RAW Paste Data

```
0100[illegible]1110[illegible]011000001101000010110001010000011010000000000000000000000001010101000100000100
0100[illegible]01000000000000000000000011000100110001110001001101000000110000000000000000
00000011000011001100[illegible]0100110111100101011000000000000000000000001010000111110000010100011000101111010011100110001111000[illegible]00000000000000001010
000100110000111000011100100011010010001100000000000000000000000010001001100101100000100010010110000010110000001100001011010011010101000100
0010001001011000001011100000010011110110001111100000000000000000000001001010001000010001001011000001100000000110000101111001101010100001000
0100010010110000011001000000100111101100011110000000000000000000000100101000100001000100101100000110100000011000011000100110101010001000
100010010110000011011000000100111101100011110000000000000000000001001010001000010001001011000010100000110101000000000000000000000101001 10
11110010101100000000000000000000010100001001100001111000100010000111000000011000100010000111100000011100011101011011100010001000011111011
01001101111001101110000000000000000000000101000000010000100010000111001101111001110000000000000000000000101001101111001101010000000000000000
```

INFECTION AND SPREADING: MALVERTISING

$$$$$$$$$$$$$$

Click here!!



Malwarebytes LABS

EXPLOITS

Canada and the U.K. hit by Ramnit Trojan in new malvertising campaign

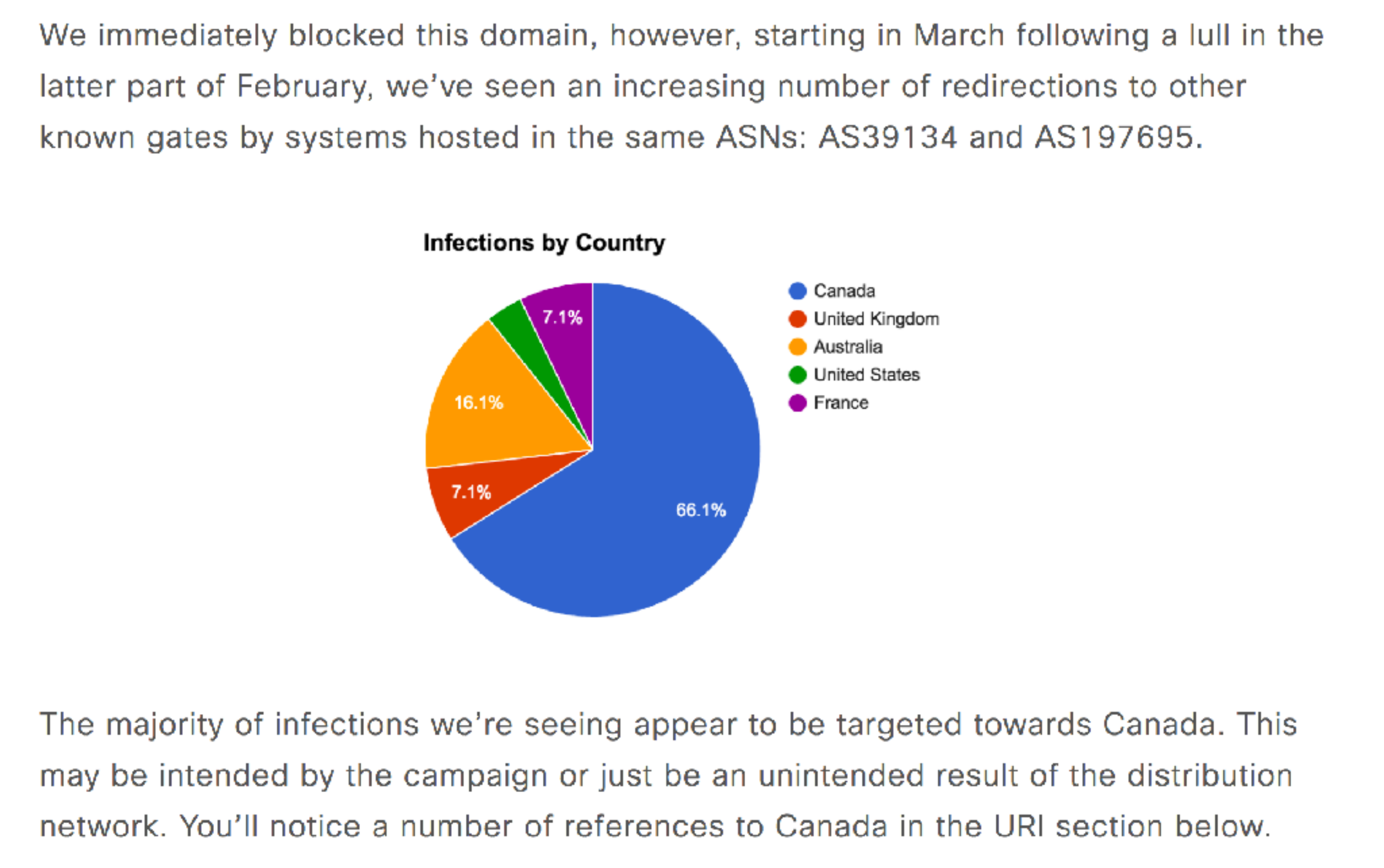
Posted: March 21, 2017 by Jérôme Segura

Over the last few days we have observed an increase in malvertising activity coming from adult websites that have significant traffic (several million monthly visits each). Malicious actors are using pop-under ads (adverts that load in a new browser window under the current active page) to surreptitiously redirect users to the RIG exploit kit.

This particular campaign abuses the ExoClick ad network (ExoClick was informed and took action to stop the fraudulent advertiser based on our reports) and, according to our telemetry, primarily targets Canada and the U.K.. The ultimate payloads we collected during this time period were all the Ramnit information stealer (banking, FTP credentials, etc.) which despite a takedown in 2015 has rebounded and is quite active again.

Pop-under ads and TDS

Pop-under ads are usually triggered when a user clicks on an item on the site they are browsing. In this particular example, clicking on one of the category thumbnails launches the pop-under window behind the main page.



We immediately blocked this domain, however, starting in March following a lull in the latter part of February, we've seen an increasing number of redirections to other known gates by systems hosted in the same ASNs: AS39134 and AS197695.

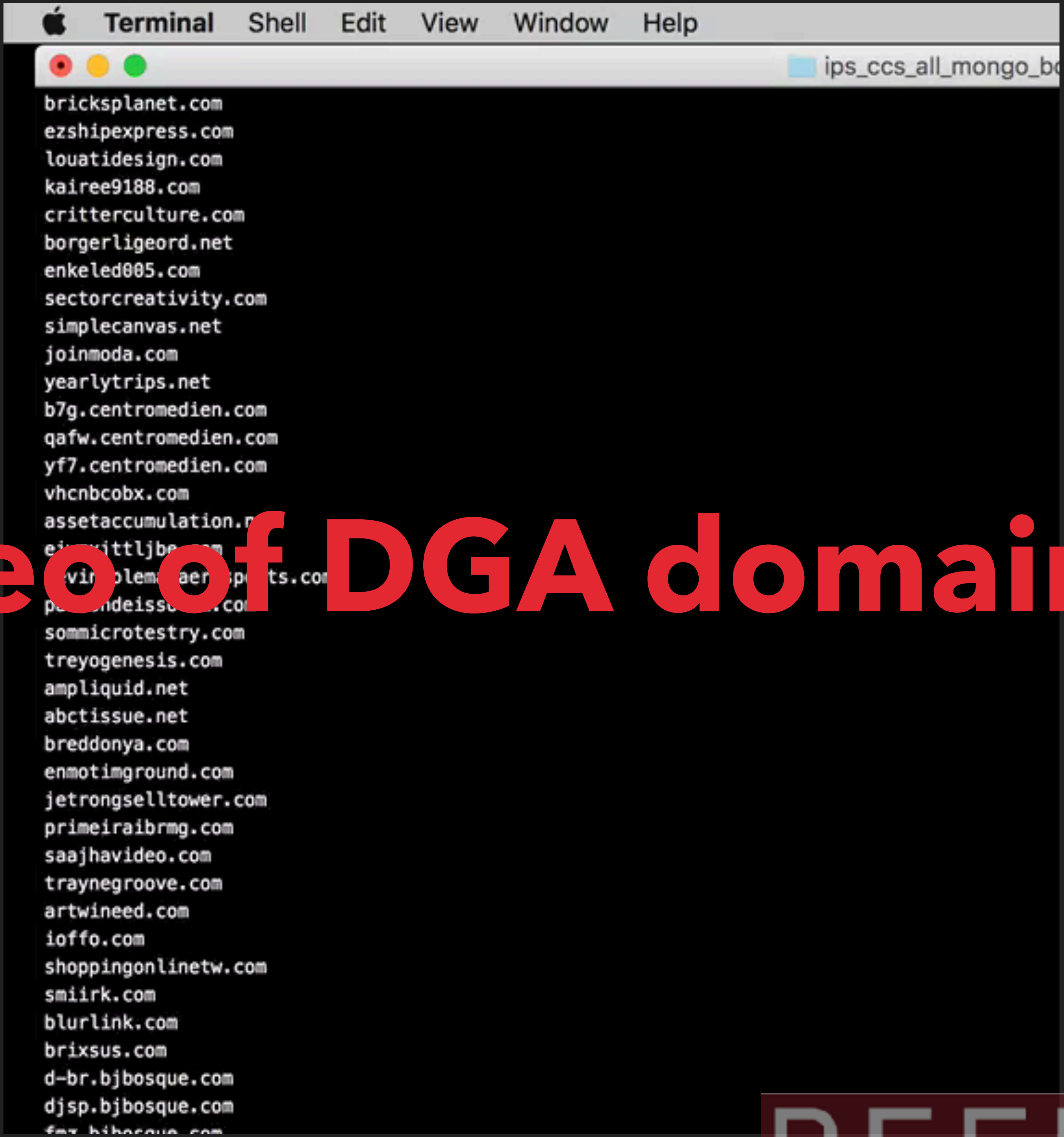
The majority of infections we're seeing appear to be targeted towards Canada. This may be intended by the campaign or just be an unintended result of the distribution network. You'll notice a number of references to Canada in the URI section below.

C&C CONTACT

C&C CONTACT – DOMAIN FLUX

- Domain Flux
  - Large amount of changing DGA domains

C&C CONTACT



```
bricksplanet.com
ezshipexpress.com
louatidesign.com
kairee9188.com
critterculture.com
borgerligeord.net
enkeled005.com
sectorcreativity.com
simplecanvas.net
joinmoda.com
yearlytrips.net
b7g.centromedien.com
qafw.centromedien.com
yf7.centromedien.com
vhcnbcobx.com
assetaccumulation.n
ei[illegible]ittljbe.com
kevincolemanaerosports.com
p[illegible]ndeisso[illegible].com
sommicrotestry.com
treyogenesis.com
ampliquid.net
abctissue.net
breddonya.com
enmotimground.com
jetrongselltower.com
primeiraibrmg.com
saajhavideo.com
traynegroove.com
artwineed.com
ioffo.com
shoppingonlinetw.com
smiirk.com
blurlink.com
brixsus.com
d-br.bjbosque.com
djsp.bjbosque.com
fmz.bjbosque.com
```

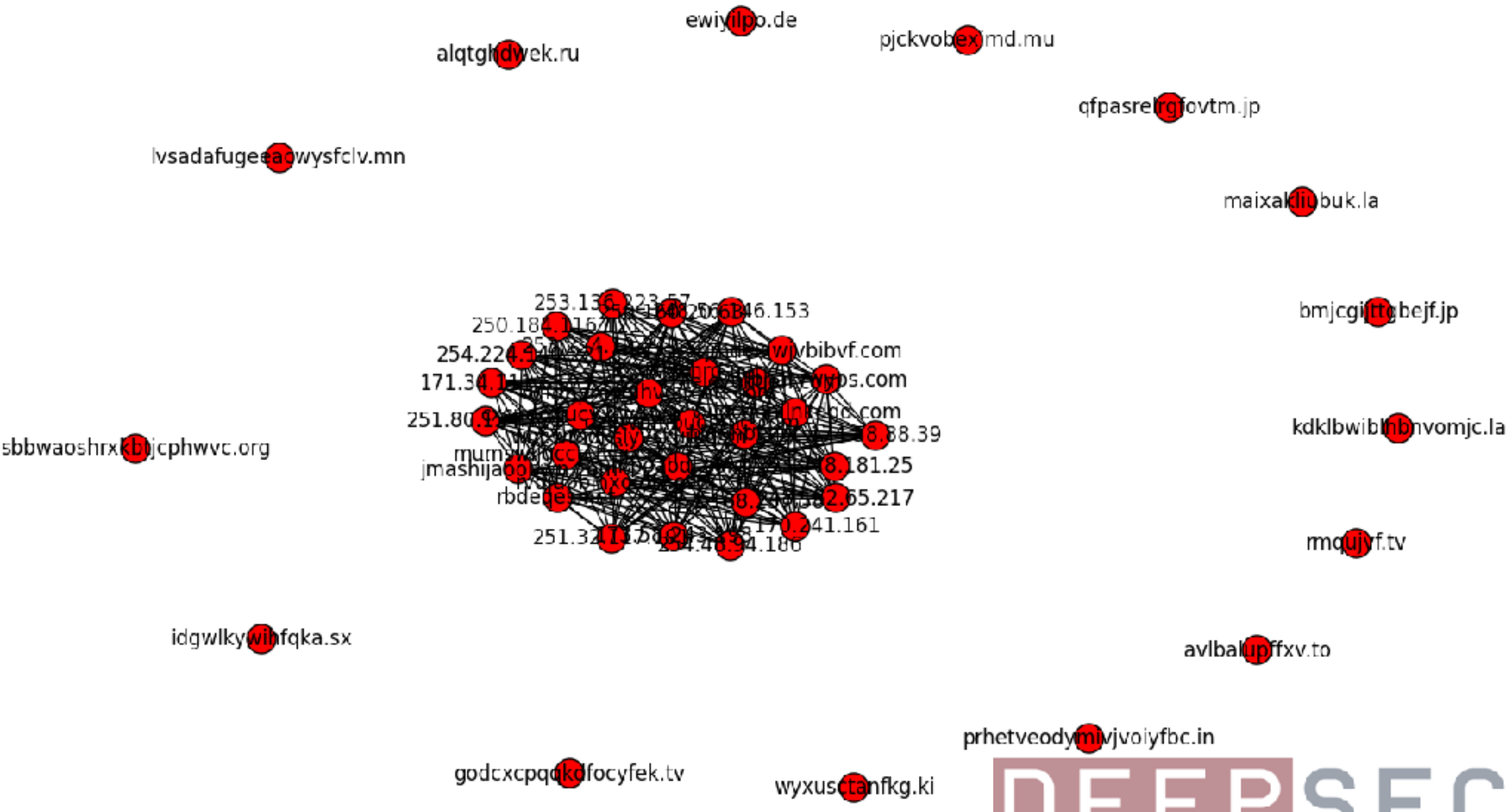
Video of DGA domains

C&C CONTACT - DOMAIN FLUX

- Domain Flux
    - Large amount of changing DGA domains
- NX Domains
    - Not all registered - lots of noise to dig through

View of NX domains

C&C CONTACT – DOMAIN FLUX



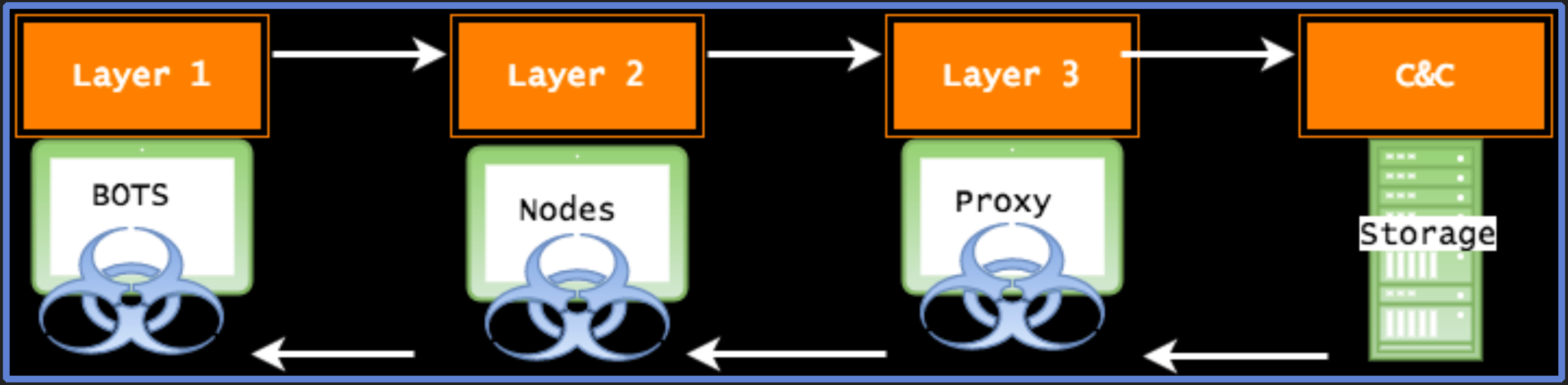
C&C CONTACT – DOMAIN FLUX

- Domain Flux
  - Large amount of changing DGA domains
- NX Domains
  - Not all registered - lots of noise to dig through
- One of the DGAs will be the C&C
- Victim beacons home - added to Botnet

C&C CONTACT

- IP FLux
  - Domain changes IPs rapidly
  - Hides behind proxy layers

EXAMPLE OF C&C CONTACT - ATTEMPTS TO STAY HIDDEN



Infected users/ computers Accept and carry out commands

More Infected Users act as HTTP proxies between bots and C&Cs

Made up of Compromised Servers. Act as proxy between Nodes & C&C Backend

C&C Backend Control Panel

REPORT & AWAIT COMMANDS

- DDoS
- Spam bot
- InfoStealer
- RAT
- Drops additional malware

MAINTAIN COMPROMISE & EVADE DETECTION

- Continues to use the techniques of fast fluxing and proxy’s to keep C&C hidden
- Staying undetected on the system
  - FullyUnDetectable - AV
  - Not making a lot of network callouts
  - Malware gains persistence on the system

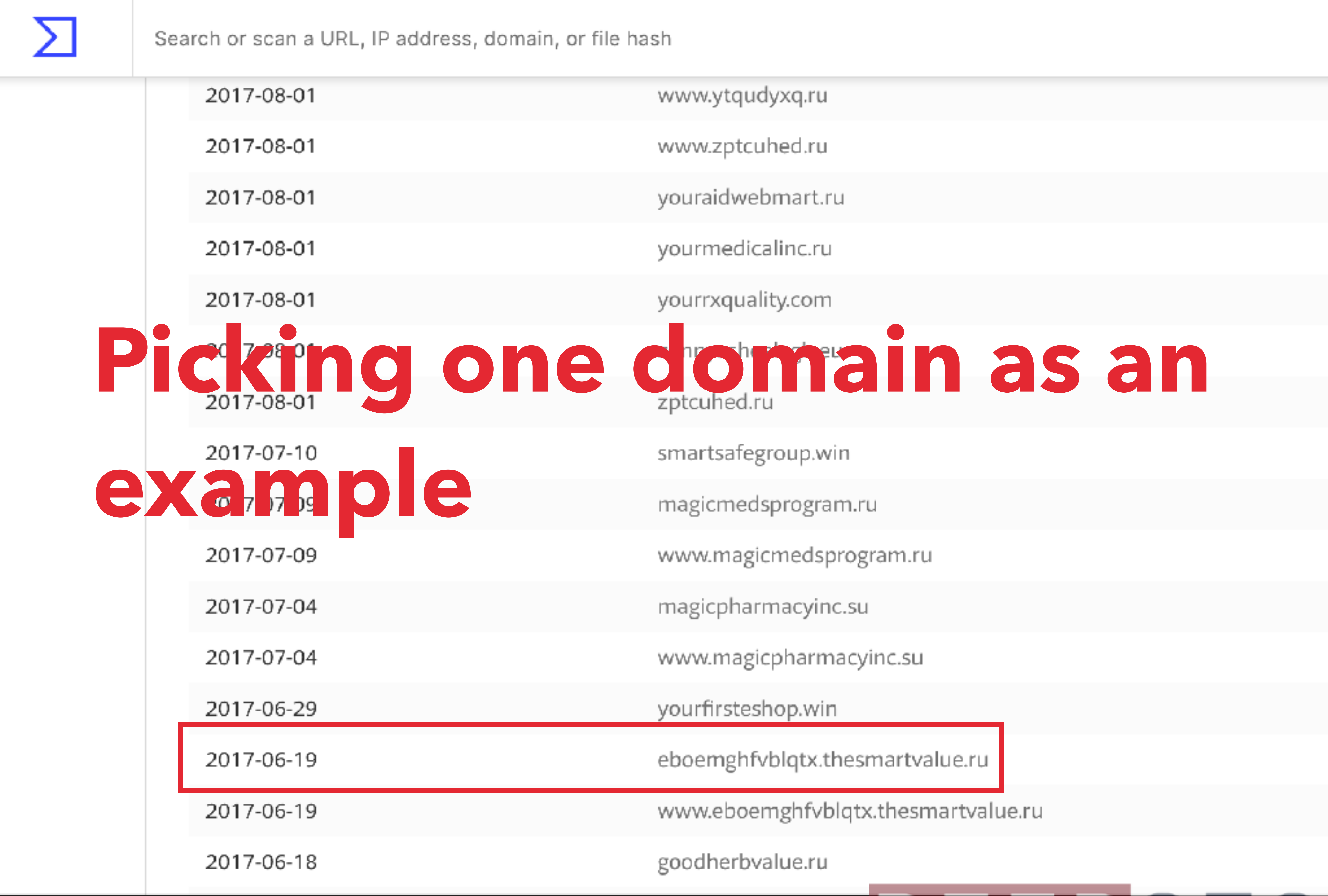
UNCOVERING INFRASTRUCTURE

PASSIVE DNS

Hailstorm Spam

95.31.22.193

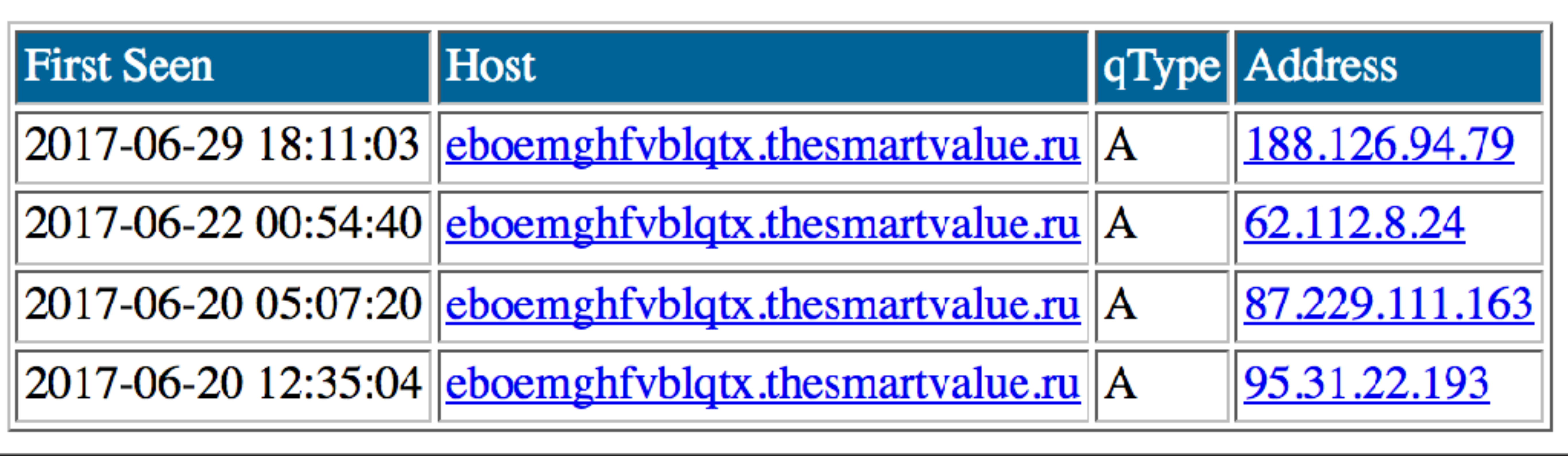
Picking one domain as an example



Search or scan a URL, IP address, domain, or file hash

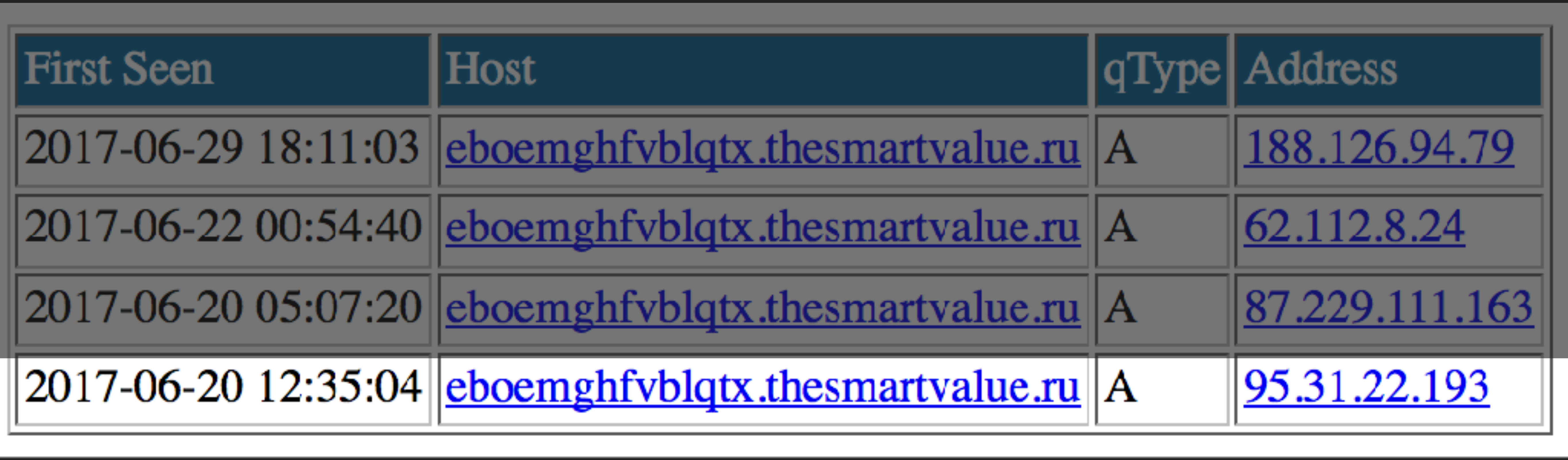
2017-08-01	www.ytqudyxq.ru
2017-08-01	www.zptcuhed.ru
2017-08-01	youraidwebmart.ru
2017-08-01	yourmedicalinc.ru
2017-08-01	yourrxquality.com
2017-08-01	[illegible]
2017-08-01	zptcuhed.ru
2017-07-10	smartsafegroup.win
2017-07-09	magicmedsprogram.ru
2017-07-09	www.magicmedsprogram.ru
2017-07-04	magicpharmacyinc.su
2017-07-04	www.magicpharmacyinc.su
2017-06-29	yourfirsteshop.win
2017-06-19	eboemghfvblqtx.thesmartvalue.ru
2017-06-19	www.eboemghfvblqtx.thesmartvalue.ru
2017-06-18	goodherbvalue.ru

Passive DNS of the IPs that domain has used

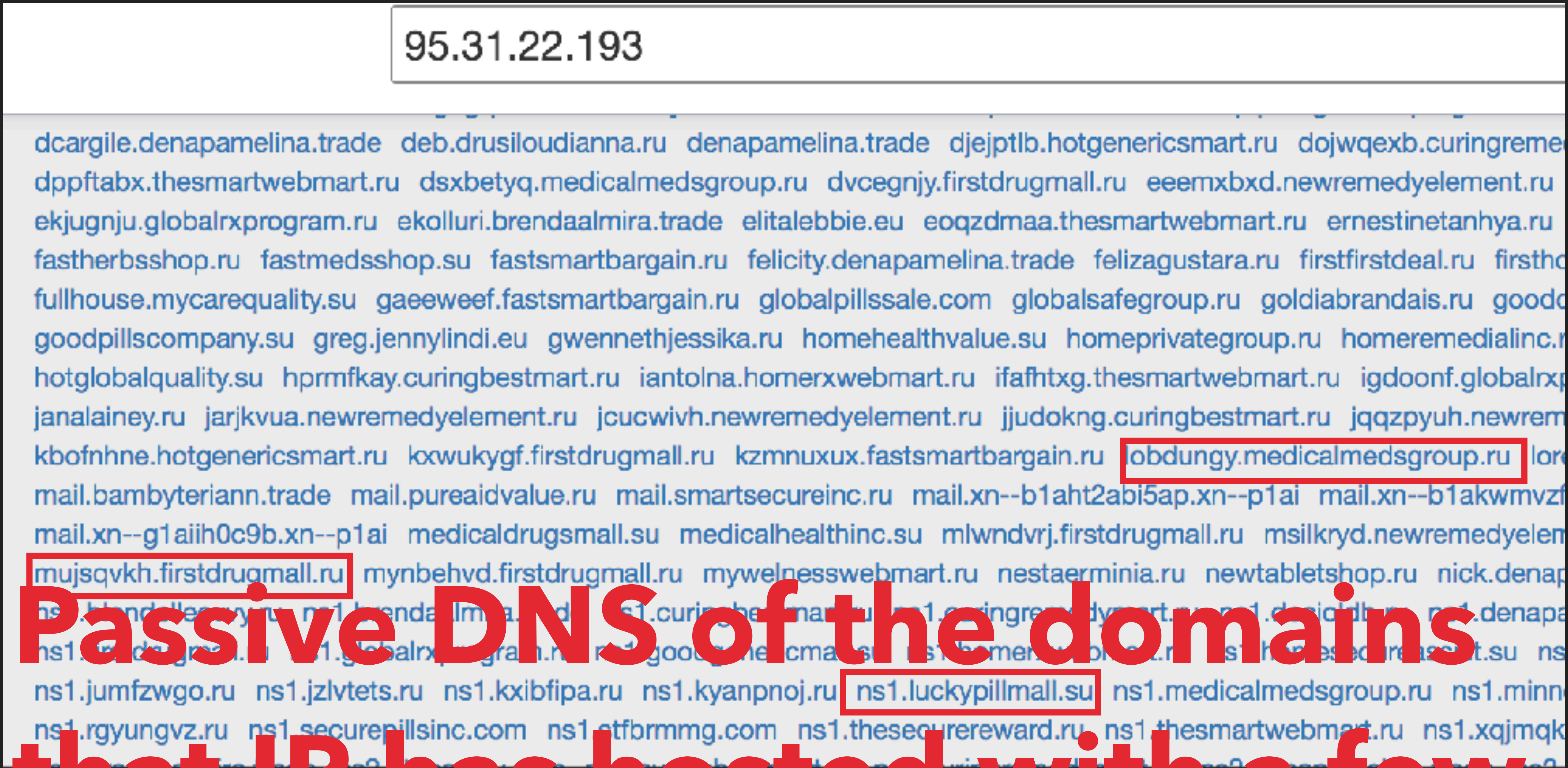


First Seen	Host	qType	Address
2017-06-29 18:11:03	eboemghfvblqtx.thesmartvalue.ru	A	188.126.94.79
2017-06-22 00:54:40	eboemghfvblqtx.thesmartvalue.ru	A	62.112.8.24
2017-06-20 05:07:20	eboemghfvblqtx.thesmartvalue.ru	A	87.229.111.163
2017-06-20 12:35:04	eboemghfvblqtx.thesmartvalue.ru	A	95.31.22.193

Passive DNS of the IPs that domain has used



First Seen	Host	qType	Address
2017-06-29 18:11:03	eboemghfvblqtx.thesmartvalue.ru	A	188.126.94.79
2017-06-22 00:54:40	eboemghfvblqtx.thesmartvalue.ru	A	62.112.8.24
2017-06-20 05:07:20	eboemghfvblqtx.thesmartvalue.ru	A	87.229.111.163
2017-06-20 12:35:04	eboemghfvblqtx.thesmartvalue.ru	A	95.31.22.193

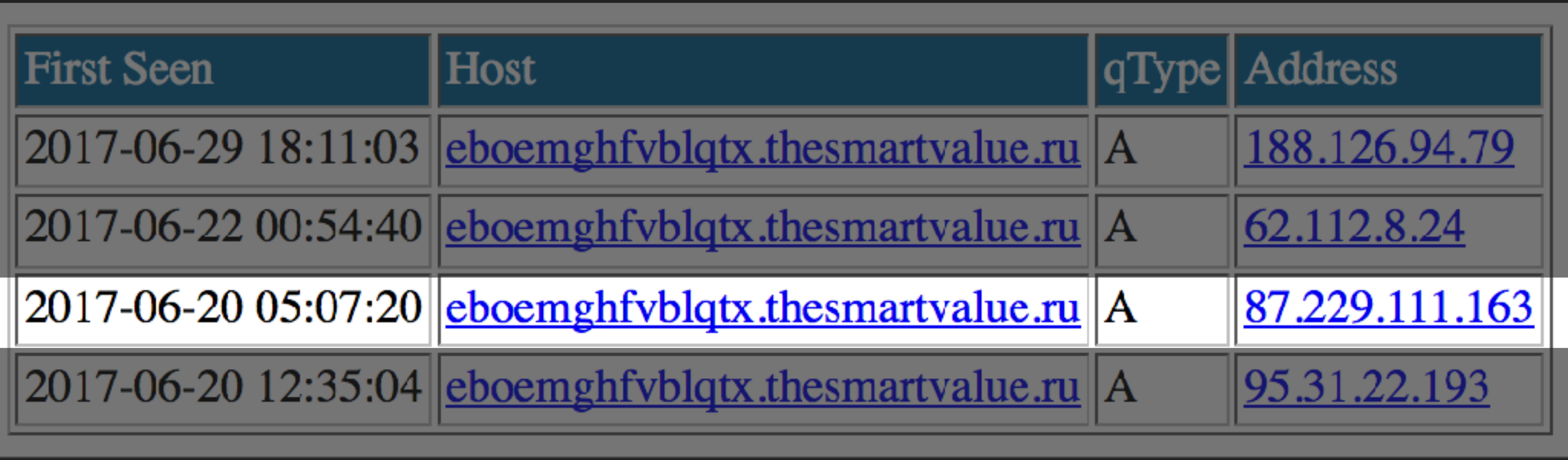


95.31.22.193

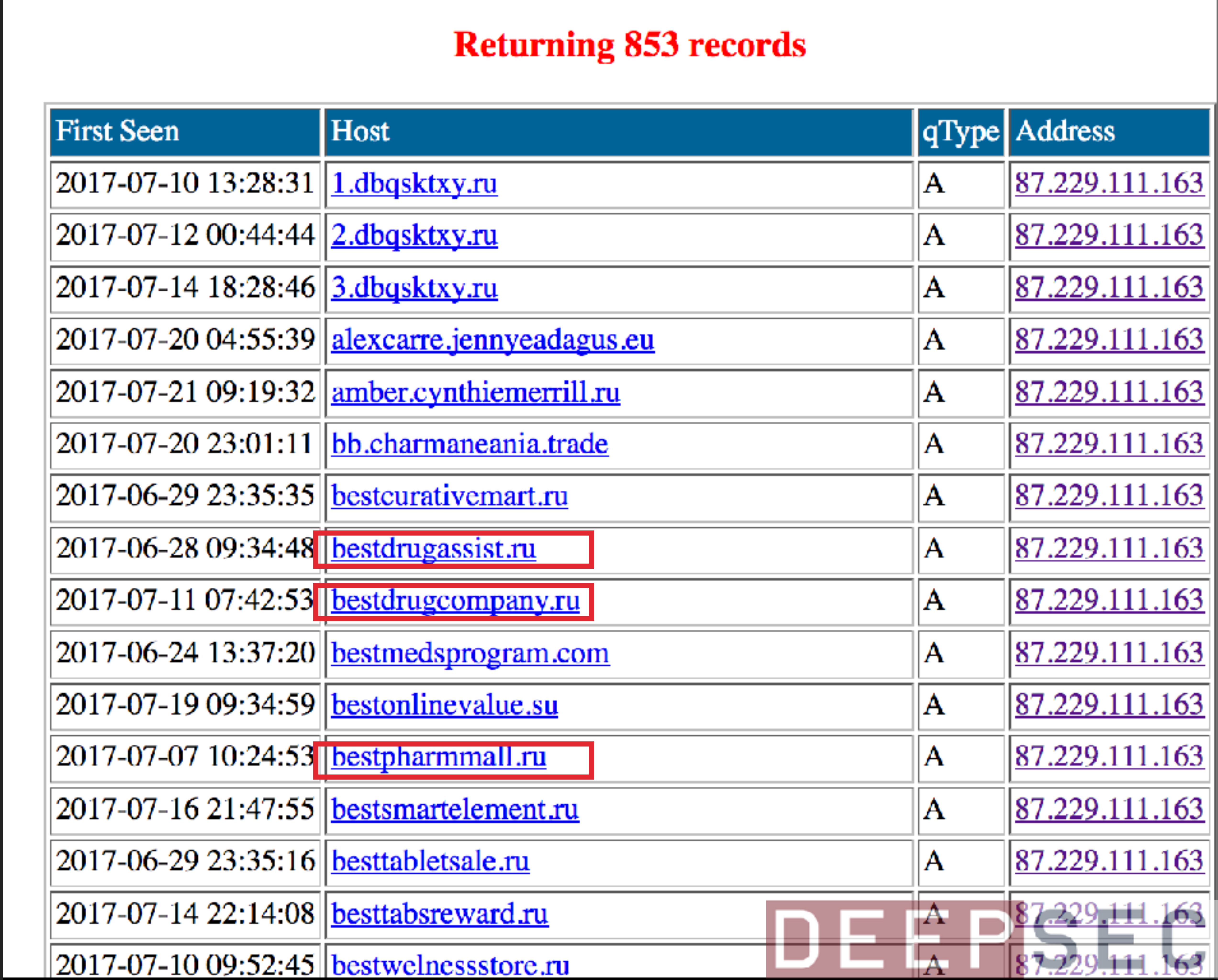
dcargile.denapamelina.trade deb.drusiloudianna.ru denapamelina.trade djejptlb.hotgenericsmart.ru dojwqexb.curingreme
dppftabx.thesmartwebmart.ru dsxbetyq.medicalmedsgroup.ru dvcegnjy.firstdrugmall.ru eeemxbxd.newremedyelement.ru
ekjugnju.globalrxprogram.ru ekolluri.brendaalmira.trade elitalebbie.eu eoqzdmaa.thesmartwebmart.ru ernestinetanhya.ru
fastherbsshop.ru fastmedsshop.su fastsmartbargain.ru felicity.denapamelina.trade felizagustara.ru firstfirstdeal.ru firsth
fullhouse.mycarequality.su gaeeweef.fastsmartbargain.ru globalpillssale.com globalsafegroup.ru goldiabrandais.ru goodc
goodpillscompany.su greg.jennylindi.eu gwennethjessika.ru homehealthvalue.su homeprivategroup.ru homeremedialinc.r
hotglobalquality.su hprmfkay.curingbestmart.ru iantolna.homerxwebmart.ru ifafhtxg.thesmartwebmart.ru igdoonf.globalrxp
janalainey.ru jarjkvua.newremedyelement.ru jcucwivh.newremedyelement.ru jjudokng.curingbestmart.ru jqqzpyuh.newrem
kbofnhne.hotgenericsmart.ru kxwukygf.firstdrugmall.ru kzmnuxux.fastsmartbargain.ru lobdungy.medicalmedsgroup.ru lore
mail.bambyteriann.trade mail.pureaidvalue.ru mail.smartsecureinc.ru mail.xn--b1aht2abi5ap.xn--p1ai mail.xn--b1akwmvzf
mail.xn--g1aiih0c9b.xn--p1ai medicaldrugsmall.su medicalhealthinc.su mlwndvrj.firstdrugmall.ru msilkryd.newremedyelem
mujsqvkh.firstdrugmall.ru mynbehvd.firstdrugmall.ru mywelnesswebmart.ru nestaerminia.ru newtabletshop.ru nick.denap
ns[illegible] ns1.brendaalmira.[illegible] ns1.curin[illegible] ns1.curingre[illegible] ns1.[illegible] ns1.denapa
ns1.[illegible] ns1.globalrx[illegible] ns1.good[illegible] ns1.homer[illegible] ns1.h[illegible]t.su ns
ns1.jumfzwgo.ru ns1.jzlvtets.ru ns1.kxibfipa.ru ns1.kyanpnoj.ru ns1.luckypillmall.su ns1.medicalmedsgroup.ru ns1.minn
ns1.rgyungvz.ru ns1.securepillsinc.com ns1.stfbrmmg.com ns1.thesecurereward.ru ns1.thesmartwebmart.ru ns1.xqjmqk

Passive DNS of the domains that IP has hosted with a few examples highlighted

Passive DNS of the another IP that domain has used

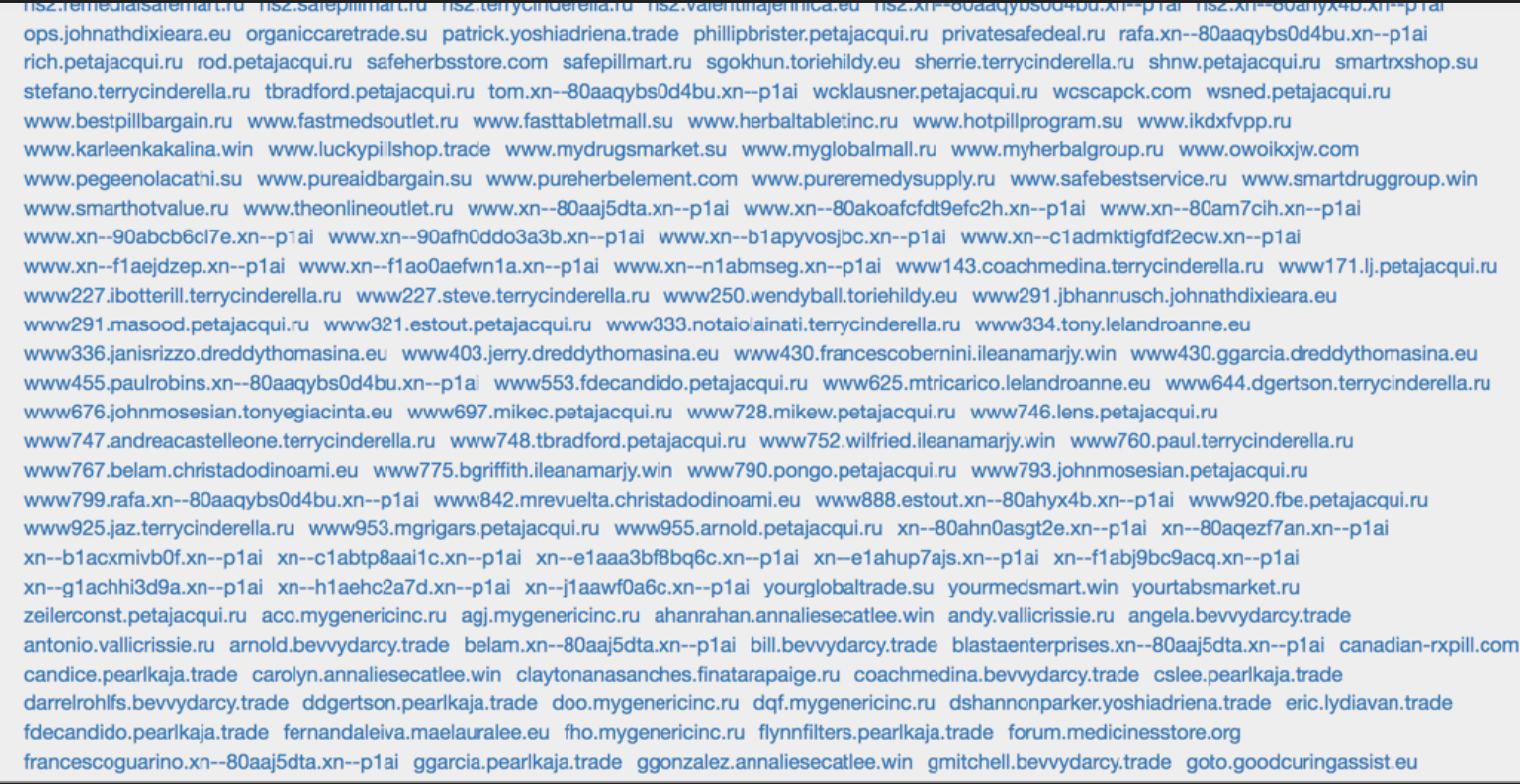


First Seen	Host	qType	Address
2017-06-29 18:11:03	eboemghfvblqtx.thesmartvalue.ru	A	188.126.94.79
2017-06-22 00:54:40	eboemghfvblqtx.thesmartvalue.ru	A	62.112.8.24
2017-06-20 05:07:20	eboemghfvblqtx.thesmartvalue.ru	A	87.229.111.163
2017-06-20 12:35:04	eboemghfvblqtx.thesmartvalue.ru	A	95.31.22.193

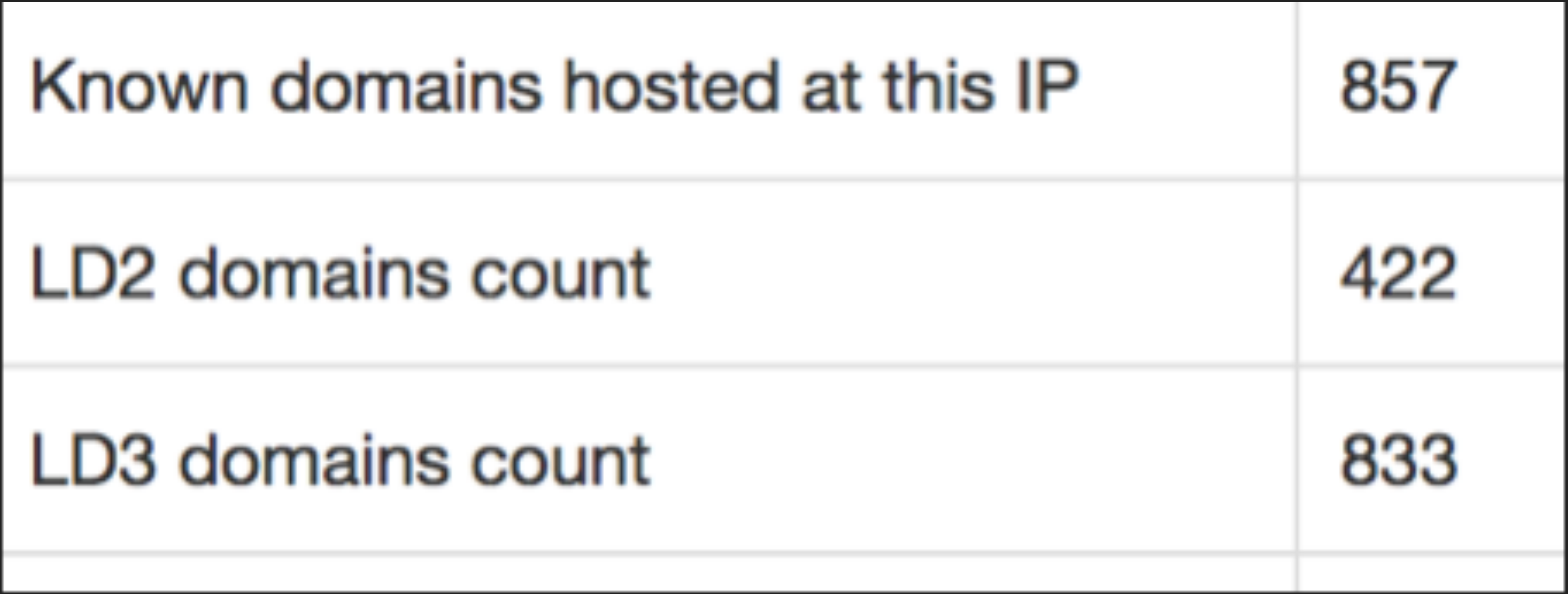


Returning 853 records

First Seen	Host	qType	Address
2017-07-10 13:28:31	1.dbqsktxy.ru	A	87.229.111.163
2017-07-12 00:44:44	2.dbqsktxy.ru	A	87.229.111.163
2017-07-14 18:28:46	3.dbqsktxy.ru	A	87.229.111.163
2017-07-20 04:55:39	alexcarre.jennyeadagus.eu	A	87.229.111.163
2017-07-21 09:19:32	amber.cynthiemerrill.ru	A	87.229.111.163
2017-07-20 23:01:11	bb.charmaneania.trade	A	87.229.111.163
2017-06-29 23:35:35	bestcurativemart.ru	A	87.229.111.163
2017-06-28 09:34:48	bestdrugassist.ru	A	87.229.111.163
2017-07-11 07:42:53	bestdrugcompany.ru	A	87.229.111.163
2017-06-24 13:37:20	bestmedsprogram.com	A	87.229.111.163
2017-07-19 09:34:59	bestonlinevalue.su	A	87.229.111.163
2017-07-07 10:24:53	bestpharmmall.ru	A	87.229.111.163
2017-07-16 21:47:55	bestsmartelement.ru	A	87.229.111.163
2017-06-29 23:35:16	besttabletsale.ru	A	87.229.111.163
2017-07-14 22:14:08	besttabsreward.ru	A	87.229.111.163
2017-07-10 09:52:45	bestwelnessstore.ru	A	87.229.111.163



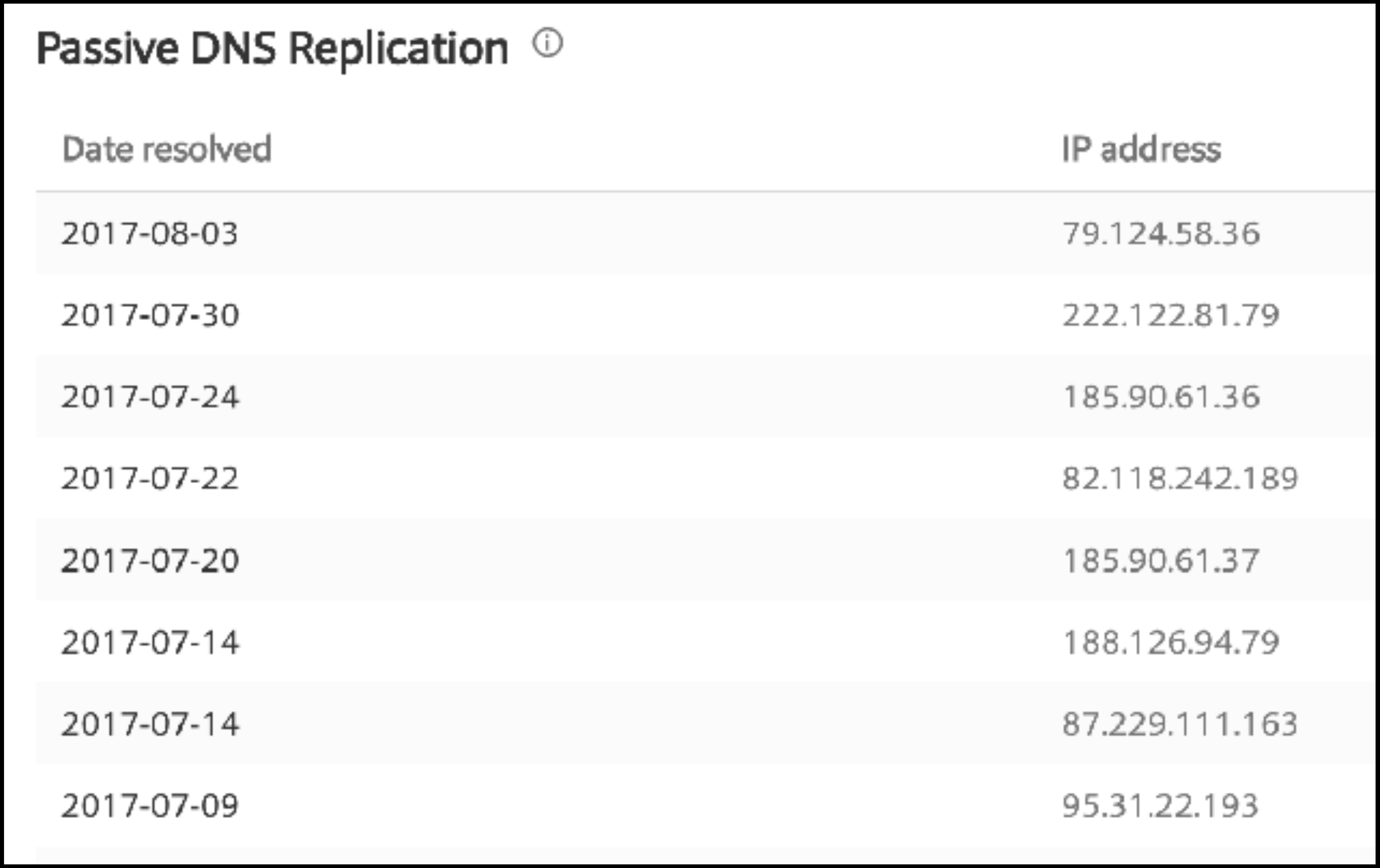
ns2.remedialsafemart.ru ns2.safepillmart.ru ns2.terrycinderella.ru ns2.valentinajennica.eu ns2.xn--80aaqybs0d4bu.xn--p1ai ns2.xn--80ahyx4b.xn--p1ai
ops.johnathdixieara.eu organiccaretrade.su patrick.yoshiadriena.trade phillipbrister.petajacqui.ru privatesafedeal.ru rafa.xn--80aaqybs0d4bu.xn--p1ai
rich.petajacqui.ru rod.petajacqui.ru safeherbsstore.com safepillmart.ru sgokhun.toriehildy.eu sherrie.terrycinderella.ru shnw.petajacqui.ru smartrxshop.su
stefano.terrycinderella.ru tbradford.petajacqui.ru tom.xn--80aaqybs0d4bu.xn--p1ai wcklausner.petajacqui.ru wcscapck.com wsned.petajacqui.ru
www.bestpillbargain.ru www.fastmedsoutlet.ru www.fasttabletmall.su www.herbaltabletinc.ru www.hotpillprogram.su www.ikdxfvpp.ru
www.karleenkakalina.win www.luckypillshop.trade www.mydrugsmarket.su www.myglobalmall.ru www.myherbalgroup.ru www.owoikxjw.com
www.pegeenolacathi.su www.pureaidbargain.su www.pureherbelement.com www.pureremedysupply.ru www.safebestservice.ru www.smartdruggroup.win
www.smarthotvalue.ru www.theonlineoutlet.ru www.xn--80aaj5dta.xn--p1ai www.xn--80akoafcfdt9efc2h.xn--p1ai www.xn--80am7cih.xn--p1ai
www.xn--90abcb6cl7e.xn--p1ai www.xn--90afh0ddo3a3b.xn--p1ai www.xn--b1apyvosjbc.xn--p1ai www.xn--c1admktigfdf2ecw.xn--p1ai
www.xn--f1aejdzep.xn--p1ai www.xn--f1ao0aefwn1a.xn--p1ai www.xn--n1abmseg.xn--p1ai www143.coachmedina.terrycinderella.ru www171.lj.petajacqui.ru
www227.ibotterill.terrycinderella.ru www227.steve.terrycinderella.ru www250.wendyball.toriehildy.eu www291.jbhannusch.johnathdixieara.eu
www291.masood.petajacqui.ru www321.estout.petajacqui.ru www333.notaiolainati.terrycinderella.ru www334.tony.lelandroanne.eu
www336.janisrizzo.dreddythomasina.eu www403.jerry.dreddythomasina.eu www430.francescobernini.ileanamarjy.win www430.ggarcia.dreddythomasina.eu
www455.paulrobins.xn--80aaqybs0d4bu.xn--p1ai www553.fdecandido.petajacqui.ru www625.mtricarico.lelandroanne.eu www644.dgertson.terrycinderella.ru
www676.johnmosesian.tonyegiacinta.eu www697.mikec.petajacqui.ru www728.mikew.petajacqui.ru www746.lens.petajacqui.ru
www747.andreacastelleone.terrycinderella.ru www748.tbradford.petajacqui.ru www752.wilfried.ileanamarjy.win www760.paul.terrycinderella.ru
www767.belam.christadodinoami.eu www775.bgriffith.ileanamarjy.win www790.pongo.petajacqui.ru www793.johnmosesian.petajacqui.ru
www799.rafa.xn--80aaqybs0d4bu.xn--p1ai www842.mrevuelta.christadodinoami.eu www888.estout.xn--80ahyx4b.xn--p1ai www920.fbe.petajacqui.ru
www925.jaz.terrycinderella.ru www953.mgrigars.petajacqui.ru www955.arnold.petajacqui.ru xn--80ahn0asgt2e.xn--p1ai xn--80aqezf7an.xn--p1ai
xn--b1acxmivb0f.xn--p1ai xn--c1abtp8aai1c.xn--p1ai xn--e1aaa3bf8bq6c.xn--p1ai xn--e1ahup7ajs.xn--p1ai xn--f1abj9bc9acq.xn--p1ai
xn--g1achhi3d9a.xn--p1ai xn--h1aehc2a7d.xn--p1ai xn--j1aawf0a6c.xn--p1ai yourglobaltrade.su yourmedsmart.win yourtabsmarket.ru
zeilerconst.petajacqui.ru acc.mygenericinc.ru agj.mygenericinc.ru ahanrahan.annaliesecatlee.win andy.vallicrissie.ru angela.bevvydarcy.trade
antonio.vallicrissie.ru arnold.bevvydarcy.trade belam.xn--80aaj5dta.xn--p1ai bill.bevvydarcy.trade blastaenterprises.xn--80aaj5dta.xn--p1ai canadian-rxpill.com
candice.pearlkaja.trade carolyn.annaliesecatlee.win claytonanasanches.finatarapaige.ru coachmedina.bevvydarcy.trade cslee.pearlkaja.trade
darrelrohlfs.bevvydarcy.trade ddgertson.pearlkaja.trade doo.mygenericinc.ru dqf.mygenericinc.ru dshannonparker.yoshiadriena.trade eric.lydiavan.trade
fdecandido.pearlkaja.trade fernandaleiva.maelauralee.eu fho.mygenericinc.ru flynnfilters.pearlkaja.trade forum.medicinesstore.org
francescoguarino.xn--80aaj5dta.xn--p1ai ggarcia.pearlkaja.trade ggonzalez.annaliesecatlee.win gmitchell.bevvydarcy.trade goto.goodcuringassist.eu



Known domains hosted at this IP	857
LD2 domains count	422
LD3 domains count	833

magicmedsprogram[.]ru that we saw on 95.31.22.193
has also resolved to **185.90.61.36**

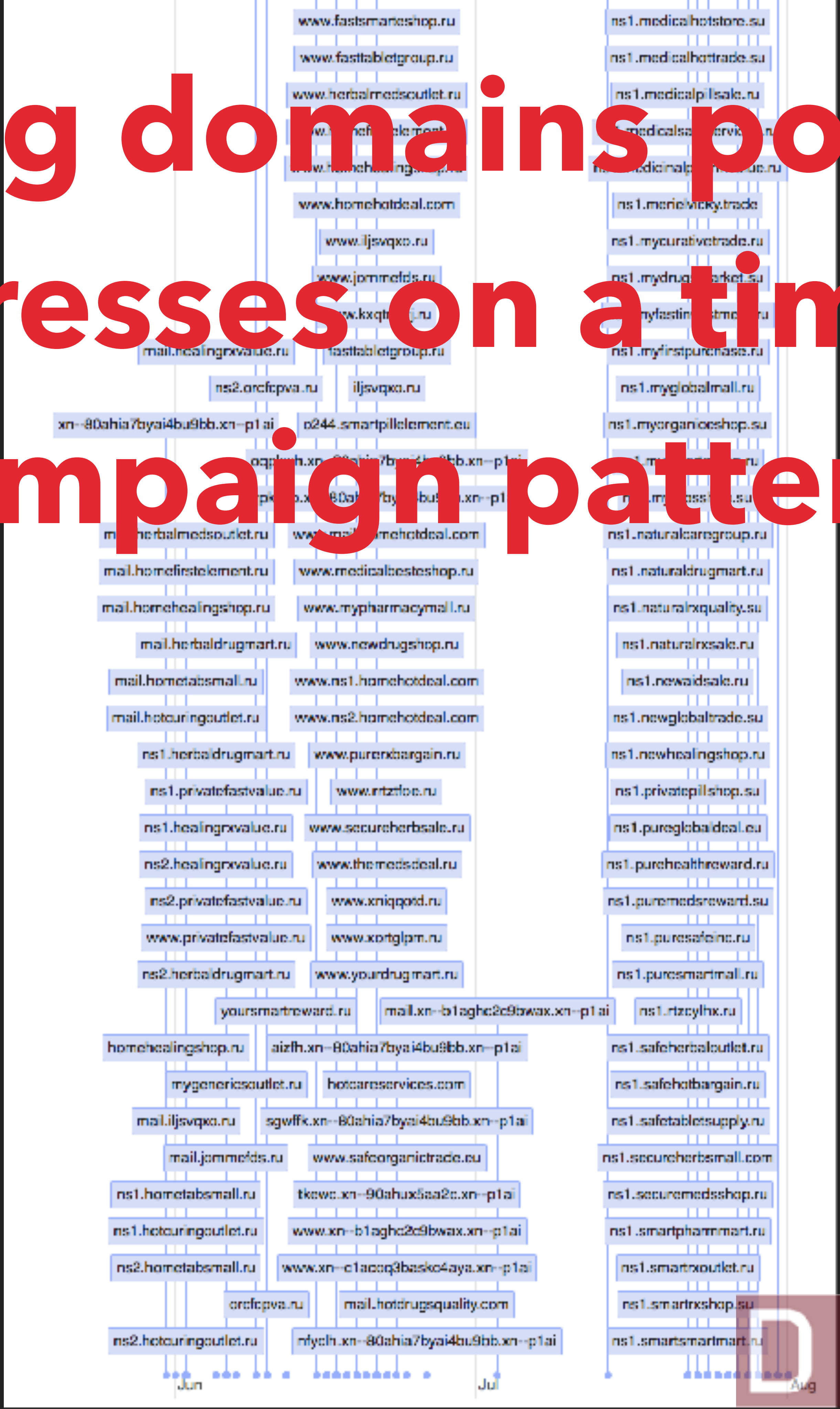
95.31.22.193
185.90.61.36
185.90.61.37
62.112.8.34
87.229.111.163
188.126.94.79
82.118.242.158
217.195.60.211
84.124.94.11



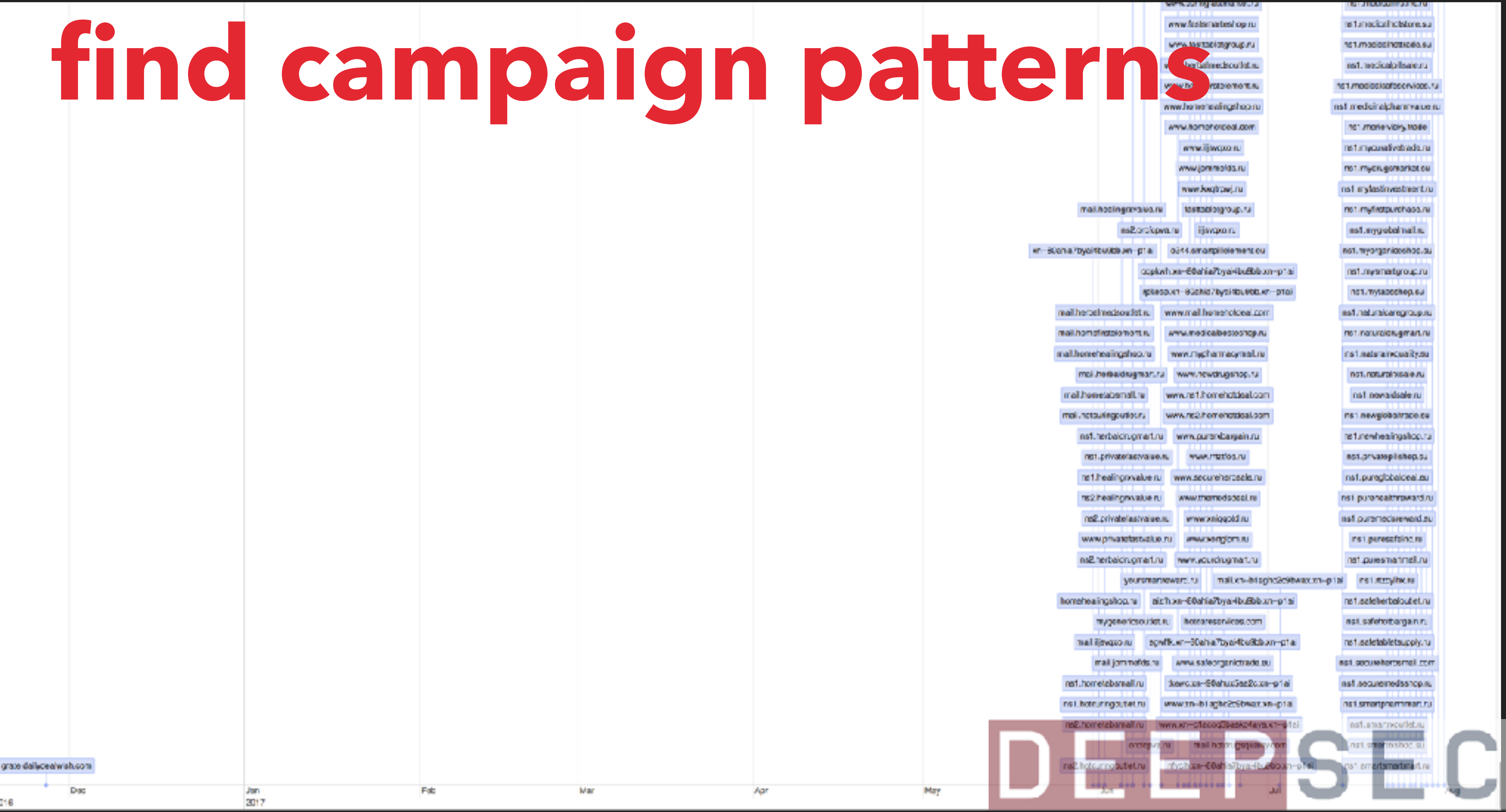
Passive DNS Replication ⓘ

Date resolved	IP address
2017-08-03	79.124.58.36
2017-07-30	222.122.81.79
2017-07-24	185.90.61.36
2017-07-22	82.118.242.189
2017-07-20	185.90.61.37
2017-07-14	188.126.94.79
2017-07-14	87.229.111.163
2017-07-09	95.31.22.193

Viewing domains pointed to IP addresses on a timeline to find campaign patterns

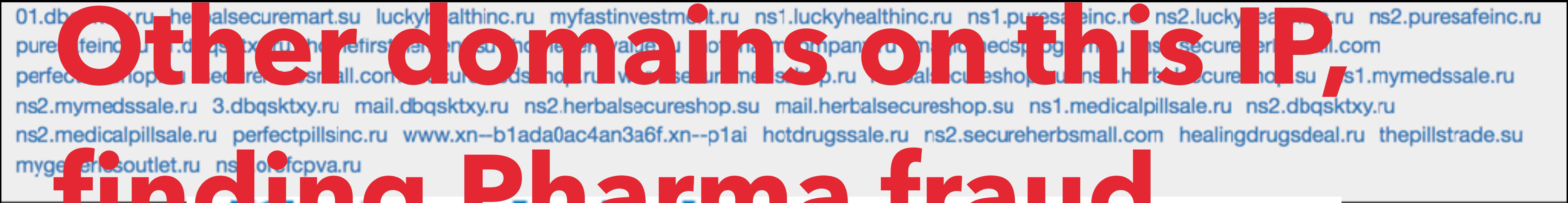


Viewing domains pointed to IP addresses on a timeline to find campaign patterns

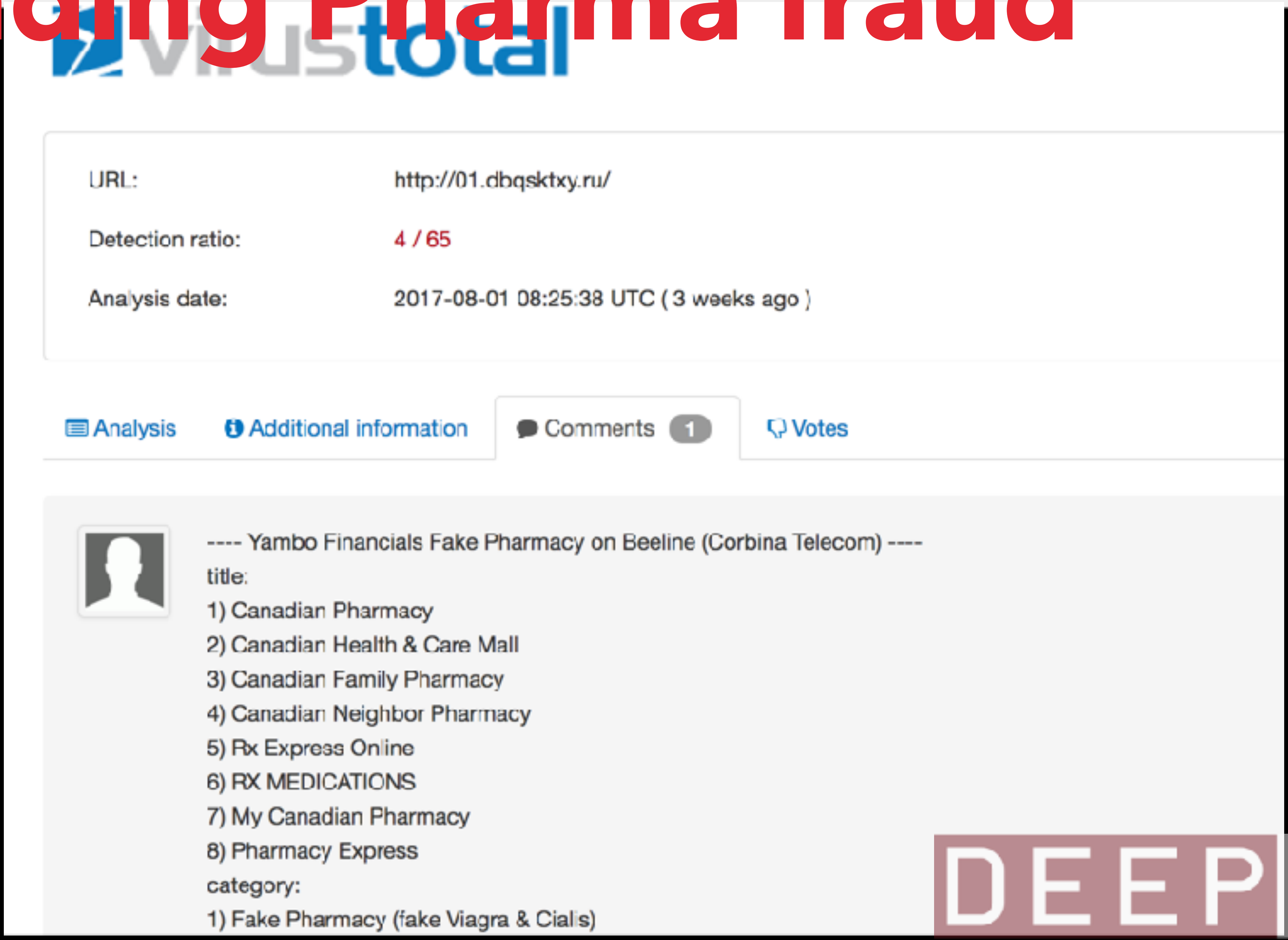


185.90.61.36

Other domains on this IP, finding Pharma fraud



01.dbqsktxy.ru herbalsecuremart.su luckyhealthinc.ru myfastinvestment.ru ns1.luckyhealthinc.ru ns1.puresafeinc.ru ns2.luckyhealthinc.ru ns2.puresafeinc.ru
puresafeinc.ru [illegible].dbqsktxy.ru [illegible]efirst[illegible] [illegible] [illegible]value.ru [illegible]company.ru [illegible]medsprog[illegible].ru [illegible]secureherbsmall.com
perfect[illegible]shop.ru secureherbsmall.com [illegible]securemedsshop.ru www.securemedsshop.ru herbalsecureshop.su ns1.herbalsecureshop.su ns1.mymedssale.ru
ns2.mymedssale.ru 3.dbqsktxy.ru mail.dbqsktxy.ru ns2.herbalsecureshop.su mail.herbalsecureshop.su ns1.medicalpillsale.ru ns2.dbqsktxy.ru
ns2.medicalpillsale.ru perfectpillsinc.ru www.xn--b1ada0ac4an3a6f.xn--p1ai hotdrugssale.ru ns2.secureherbsmall.com healingdrugsdeal.ru thepillstrade.su
mygenericsoutlet.ru ns[illegible]orefcpva.ru



URL: http://01.dbqsktxy.ru/

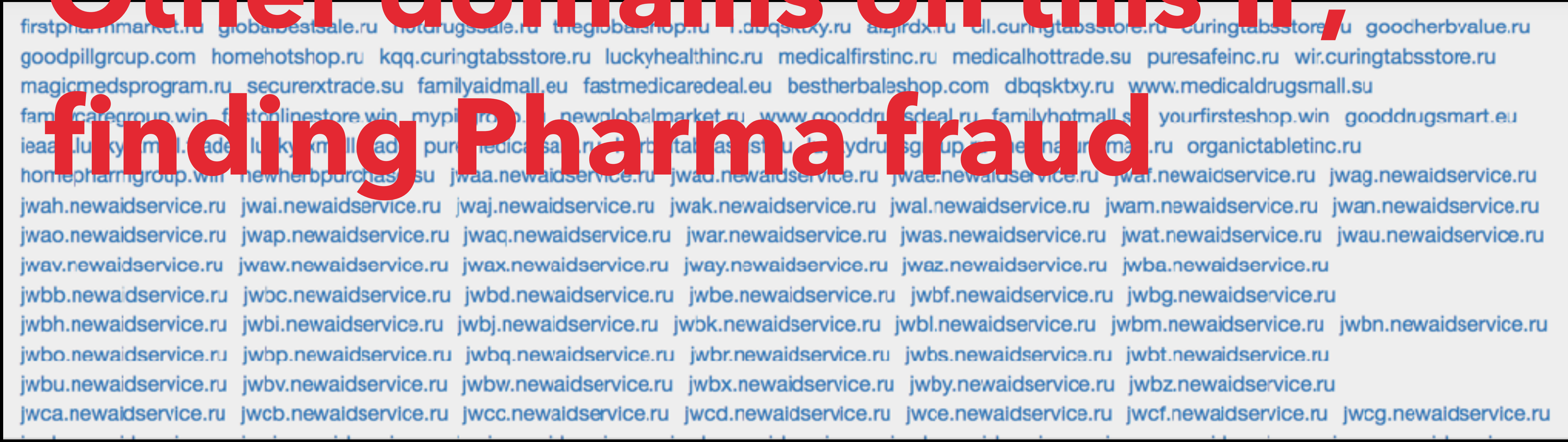
Detection ratio: 4 / 65

Analysis date: 2017-08-01 08:25:38 UTC (3 weeks ago)

---- Yambo Financials Fake Pharmacy on Beeline (Corbina Telecom) ----
title:
1) Canadian Pharmacy
2) Canadian Health & Care Mall
3) Canadian Family Pharmacy
4) Canadian Neighbor Pharmacy
5) Rx Express Online
6) RX MEDICATIONS
7) My Canadian Pharmacy
8) Pharmacy Express
category:
1) Fake Pharmacy (fake Viagra & Cialis)

217.195.60.211

Other domains on this IP, finding Pharma fraud



firstpharmmarket.ru globalbestsale.ru hotdrugssale.ru theglobalshop.ru [illegible].dbqsktxy.ru aizjirdx.ru dll.curingtabsstore.ru curingtabsstore.ru goodherbvalue.ru goodpillgroup.com homehotshop.ru kqq.curingtabsstore.ru luckyhealthinc.ru medicalfirstinc.ru medicalhottrade.su puresafeinc.ru wir.curingtabsstore.ru magicmedsprogram.ru securerxtrade.su familyaidmall.eu fastmedicaredeal.eu bestherbaleshop.com dbqsktxy.ru www.medicaldrugsmall.su familycaregroup.win firstonlinestore.win mypillgroup.[illegible] newglobalmarket.ru www.gooddrugsdeal.ru familyhotmall.su yourfirsteshop.win gooddrugsmart.eu ieaa[illegible].luckyxmall.trade luckyxmall.trade puremedicalsale.ru [illegible] luckydrugsgroup.ru [illegible].ru organictabletinc.ru homepharmgroup.win newherbpurchase.su jwaa.newaidservice.ru jwad.newaidservice.ru jwae.newaidservice.ru jwaf.newaidservice.ru jwag.newaidservice.ru jwah.newaidservice.ru jwai.newaidservice.ru jwaj.newaidservice.ru jwak.newaidservice.ru jwal.newaidservice.ru jwam.newaidservice.ru jwan.newaidservice.ru jwao.newaidservice.ru jwap.newaidservice.ru jwaq.newaidservice.ru jwar.newaidservice.ru jwas.newaidservice.ru jwat.newaidservice.ru jwau.newaidservice.ru jwav.newaidservice.ru jwaw.newaidservice.ru jwax.newaidservice.ru jway.newaidservice.ru jwaz.newaidservice.ru jwba.newaidservice.ru jwbb.newaidservice.ru jwbc.newaidservice.ru jwbd.newaidservice.ru jwbe.newaidservice.ru jwbf.newaidservice.ru jwbg.newaidservice.ru jwbh.newaidservice.ru jwbi.newaidservice.ru jwbj.newaidservice.ru jwbk.newaidservice.ru jwbl.newaidservice.ru jwbm.newaidservice.ru jwbn.newaidservice.ru jwbo.newaidservice.ru jwbp.newaidservice.ru jwbq.newaidservice.ru jwbr.newaidservice.ru jwbs.newaidservice.ru jwbt.newaidservice.ru jwbu.newaidservice.ru jwbv.newaidservice.ru jwbw.newaidservice.ru jwbx.newaidservice.ru jwby.newaidservice.ru jwbz.newaidservice.ru jwca.newaidservice.ru jwcb.newaidservice.ru jwcc.newaidservice.ru jwcd.newaidservice.ru jwce.newaidservice.ru jwcf.newaidservice.ru jwcg.newaidservice.ru

=

```
"09f1d49065108a595578ff86ff63a514d47d5496ab5c23f38cda1f0d57dd6cd1", "bb0881b7179033710d26beded4f69a9a8b80702f", "e9a81fb5fd86ba9a78ec6528c2b1ae37"
"7fd77297808d78a1fd4ae950dfff96cebc2f9be779d831c4367c427a23f1eb7e", "e8dbf5f13bc315dbdb3edf73e110f1970a575edb", "66c44550391b3390b4487c625e046173"
"b4ffc48d7ce966631d1a7eba54f91047c979f53211ce077f528068adb2140cf2", "7f3047178883c92acc799a9b7be2dba1d9e6c346", "e0a5aaa4319e09cca2d05c44797559d3"
"864a3f9899e9a0420b34ab16de2e0085a06a9c7fbe7ec548cd3e15b0c5feb2f0", "90987b26896ed9451e[illegible]a6ef5069f16532348922", "7ee21f336027270cd2ce9b087c261059"
"6ec83b8226a492f41175322003ed6183b41c2c4541d5193bded0f9851876b2a3", "a2e3dc7a7e65c3256f[illegible]b98127405d469089609c", "3e31da2e063090a016ef4a3cef79cbfd"
"64ea76d8ef8cb13f249eddb382ee998d2ab7e6ff32655105b5efdbbc6eea450a", "8755924b69af[illegible]765b157d8fbb13fedb47", "f548ab42e92d25959f5dbc0d4f01a635"
"58f519c6d9db704df9a5a0b697f727238db5cfc9e7ce5fb0d8d49a40bc6cf2f8", "d7b8132ee[illegible]abecc2[illegible]22243373c5876311e8b", "e613cf78955a4c1d8732b0ecb202caec"
"4bd06baf053614a9ef561779097b672db28caf2f31ce2346ed88e03439ebc305", "90e3230[illegible]add246c60[illegible]7ddfe73f92763f228f0", "549a242c84d00a4fee0580b396ddfa31"
"47c79e706903a773ba20d94136ac10542f4342d2a387392e6edcf130ee96ddfa", "285b[illegible]dfdd12a6858[illegible]203bdcbfb9dd12a86b3", "70d6764da826e1b4180af95bbf1ffd59"
"368834d7d5319d94da43946d0d290841d8d0f74a5856b6a46f504559b5fd372d[illegible]841[illegible]c6af89492a3d19edd6ed8b22a", "0acaa22f146196f5eaaecd3a4ca18232"
"16933d9e56416ef25096276c66417fea20f6ba68fe0695eb6a9a0d4175db47c[illegible]", "9bbe06b[illegible]5b864[illegible]e125d90d9e3da1ce0b477802", "0bc6a973616eff0ecd2d956b464b8ec2"
"0c619cc80a3a68864010531c5fa0eded2a616b1799d23740a7aa4cb4c83f4[illegible]7", "2677[illegible]96[illegible]97fe56733dff4d88cfb4e088f494d1", "f9dbc99e389beecbc09e4fed32b63dcd"
"c74b5b0183e4f1c4f85d9714bfeaa311d57c36827c8e3ef473529[illegible]e1[illegible]", "df5d[illegible]9eae8304bac9acdf73958f3357e831fd29", "918c69dbb4f2f5d16618c3d33d3a1706"
"61ab284b33d34fedb4725c0c3e5e1a2a4a3cc3767f29b10b87d[illegible]98bf[illegible]47[illegible]", "27[illegible]bf1138e546adfd70e81a125d3b10d5a14897", "85875718160f86a6b2a50befab250f43"
"6319733d3790d21f9f312319c6f87d4d7bdb7a3fe998eb74df9[illegible]6e61dd7[illegible]03", "3aa9f817ab594f8cf66d1fd8cc505b6417ed04a8", "4b3168714b43b7e17453ec3e17f6cf5b"
"6eeb0454bf825824cf528859da0cf3b69dee10b4d69313ba66db[illegible]90cbe9[illegible]c", "4325e522e6297e754795aa4c90ade1305e950e7d", "5ec24081bd392430abd20d3213826bf2"
"fba0d7b1db1d0770f23eecf1e42875aa04c330fec2[illegible]6f6ab040[illegible]964", "2c4552736fcd368d4dd1169e6f4c3c0cb69f21d6", "bfe7965da54f2b26d384ebc1fe7cfd07"
"ed884cc38b4b99e1bcdaf65fd07b40f01168926264bf[illegible]4e866ed3547175229", "a7de4c60611719d9d9c13c82b6b09523b1028dd4", "2aa3ecc4d16529567d5feadde6472f0f"
"2e16d36064f2048f529d220d2cb3ce6ce0dccfdcd05d7[illegible]818[illegible]69f9bcd38f", "2f4fddd232ab44c0ae74fba4aee01e5714ad0c4e", "8fd9c646df2d7d03259a8d0124673355"
"c5be[illegible]05090f07ba8aaecc55ecb63[illegible]726a7e565cd6a73[illegible]c4d[illegible]708aeaa1", "35fb6e3c4839e7281ce67c8cabfdfa7f2e[illegible]380c4", "[illegible]cb3067d72959dab3f2465f83ecbd3641"
"[illegible]38[illegible]634[illegible]67d[illegible]8b947[illegible]60c[illegible]25[illegible]f664[illegible]e244647[illegible]45f[illegible]4", "[illegible]a67[illegible]0ab[illegible]5157f[illegible]742[illegible]e8dd", "[illegible]b26dd093"
"112[illegible]805[illegible]deb8be[illegible]fd[illegible]0769[illegible]ffbe[illegible]06d7[illegible]0b3[illegible]f5[illegible]41", "0d[illegible]b48[illegible]86[illegible]ad9[illegible]da1[illegible]3df8", "72[illegible]17a[illegible]e5[illegible]90[illegible]14[illegible]57[illegible]abd49"
"7e9a[illegible]9e[illegible]a5d[illegible]ab49b2[illegible]a3[illegible]01[illegible]2a56[illegible]a5[illegible]0fd97[illegible]d[illegible]ccf4[illegible]", "0[illegible]ec0[illegible]1c[illegible]9c[illegible]48[illegible]2c2[illegible]e0040[illegible]", "2a[illegible]90b[illegible]20[illegible]76[illegible]b1[illegible]35f0191a"
"5527ab9e407e[illegible]260f695776c419d8b52c9c70d4e30666fc37c66d217fdffe73", "b6241[illegible]4ed0804[illegible]7c603b9eb360e7cf836b11fd43", "d2e8d8f37b9fdf0717522c9c9173b367"
"491281be556[illegible]50f171e4334972a7dd09eee28acd24a5274dd7d7787100beb37", "a5e5[illegible]e1115e2[illegible]b58c2c4432b519aa0adafec970", "39af562ed60ceb490cc0fe4a195caf1d"
```

LOCKY

Locky also dropped from these domains

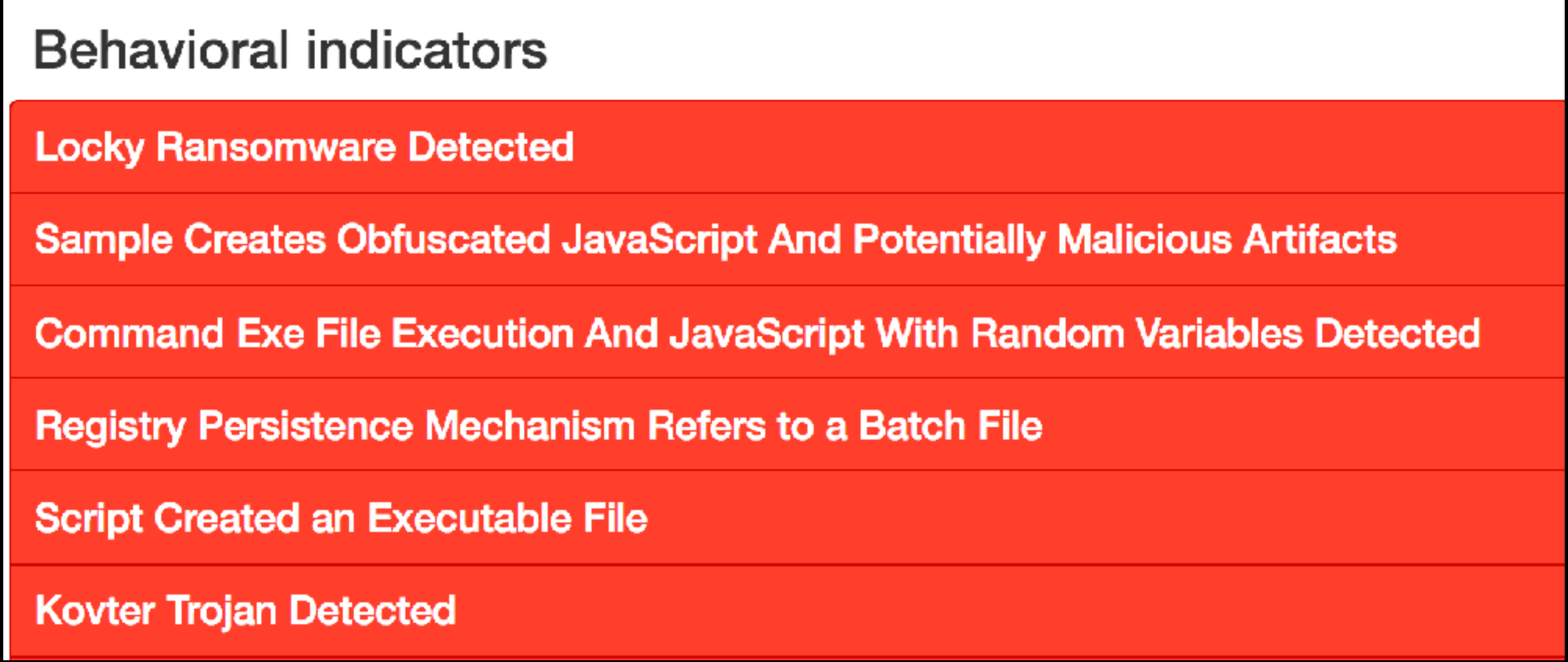
e0e59486e2c61c17ea4ed4a2efcd6deb6e6398
88715225d4b38521473212c438

UPS-Delivery-007879129.doc.zip

Locky also dropped from these domains

**e0e59486e2c61c17ea4ed4a2efcd6deb6e6398
88715225d4b38521473212c438**

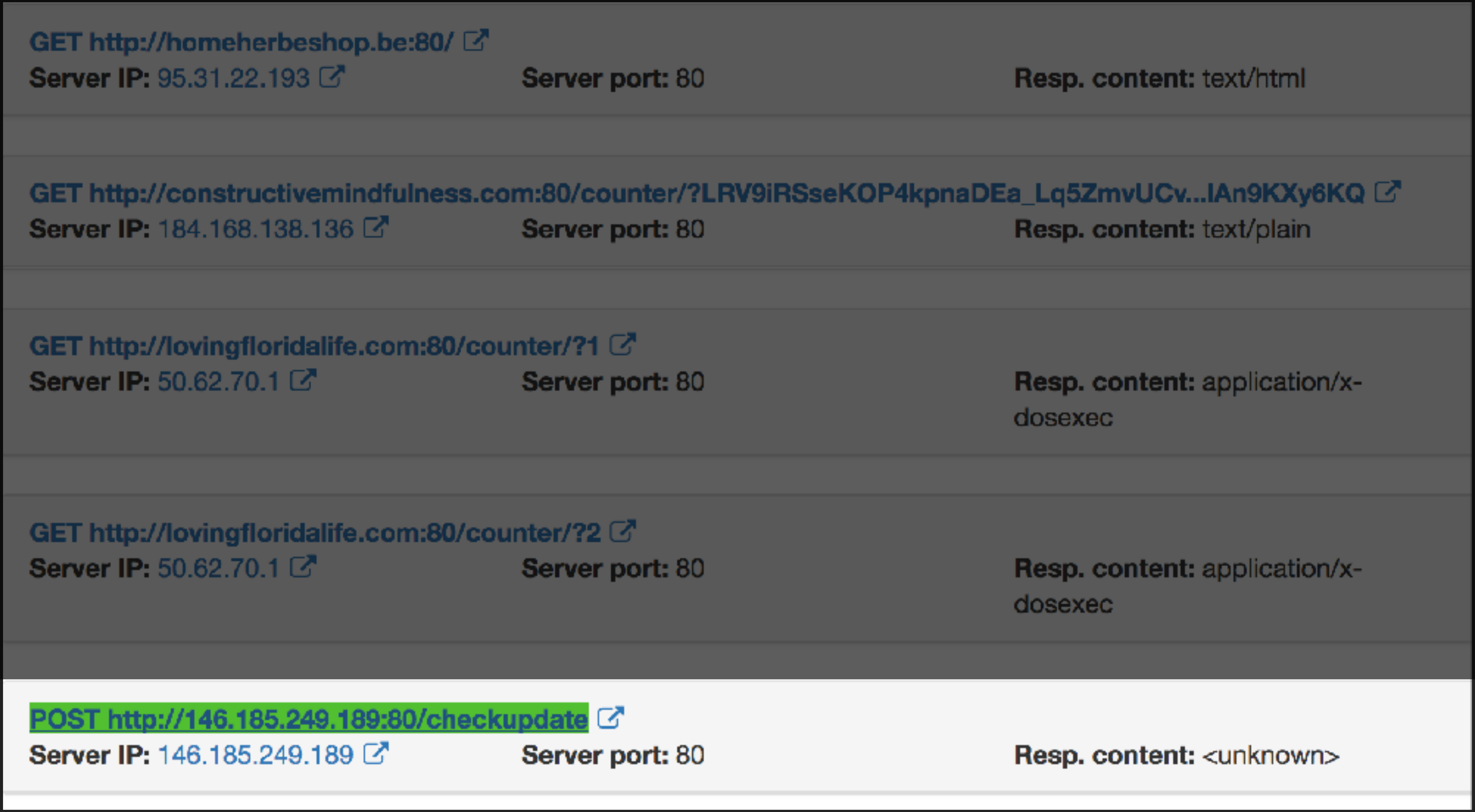
UPS-Delivery-007879129.doc.zip



Behavioral indicators

- Locky Ransomware Detected
- Sample Creates Obfuscated JavaScript And Potentially Malicious Artifacts
- Command Exe File Execution And JavaScript With Random Variables Detected
- Registry Persistence Mechanism Refers to a Batch File
- Script Created an Executable File
- Kovter Trojan Detected

C&C Server Contact



GET http://homeherbeshop.be:80/

Server IP: 95.31.22.193 Server port: 80 Resp. content: text/html

GET http://constructivemindfulness.com:80/counter/?LRV9iRSseKOP4kpnaDEa_Lq5ZmvUCv...IAn9KXy6KQ

Server IP: 184.168.138.136 Server port: 80 Resp. content: text/plain

GET http://lovingfloridalife.com:80/counter/?1

Server IP: 50.62.70.1 Server port: 80 Resp. content: application/x-dosexec

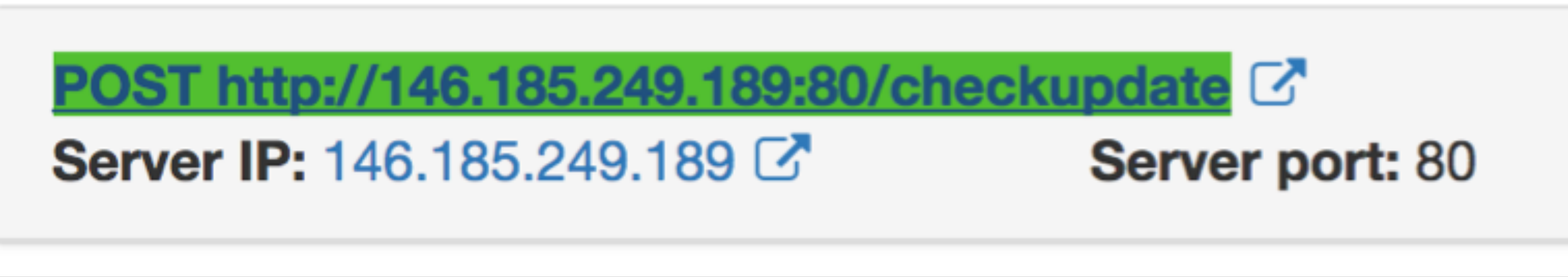
GET http://lovingfloridalife.com:80/counter/?2

Server IP: 50.62.70.1 Server port: 80 Resp. content: application/x-dosexec

POST http://146.185.249.189:80/checkupdate

Server IP: 146.185.249.189 Server port: 80 Resp. content: <unknown>

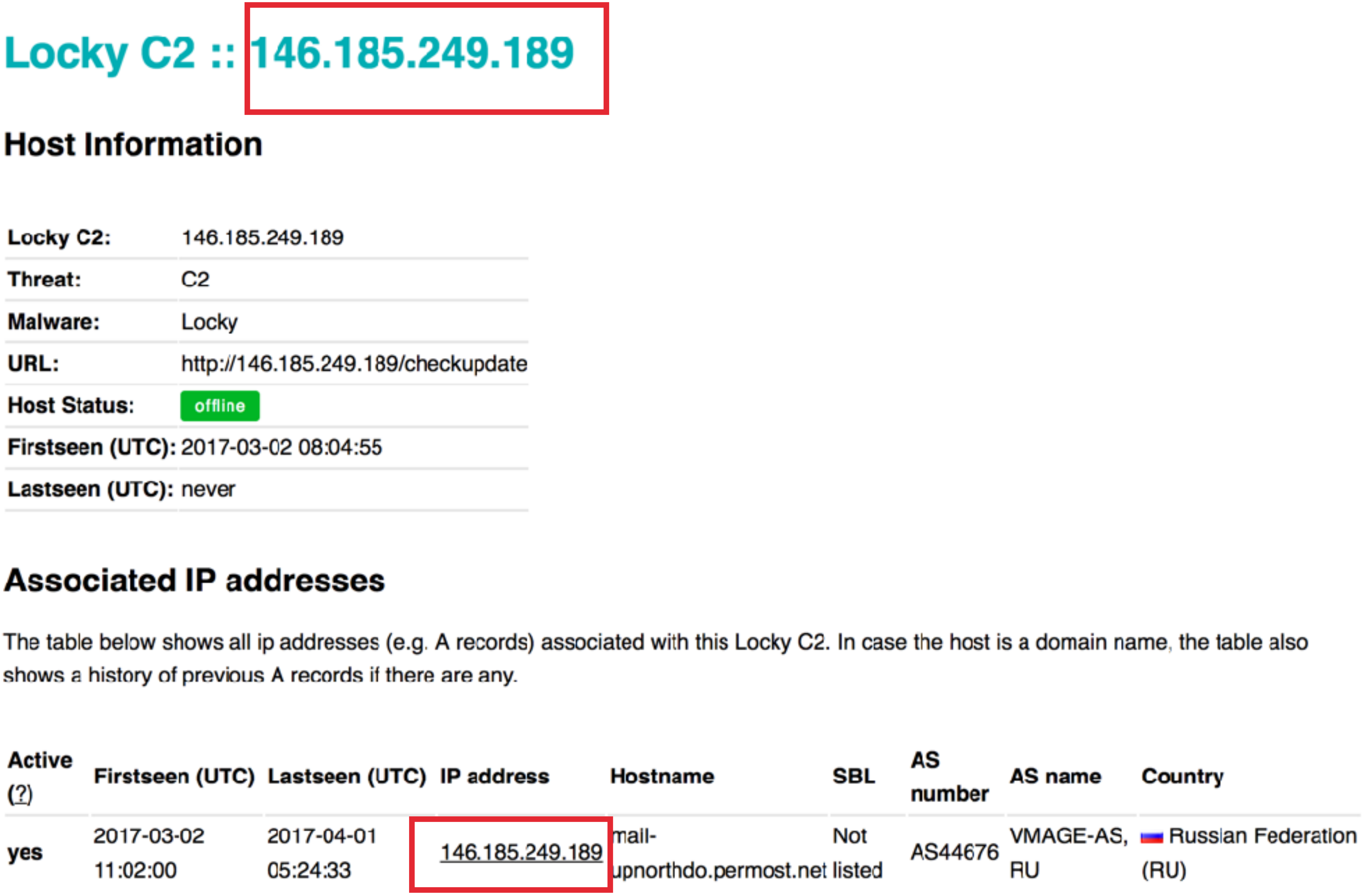
C&C Server Contact



POST http://146.185.249.189:80/checkupdate

Server IP: 146.185.249.189

Server port: 80



Locky C2 :: 146.185.249.189

Host Information

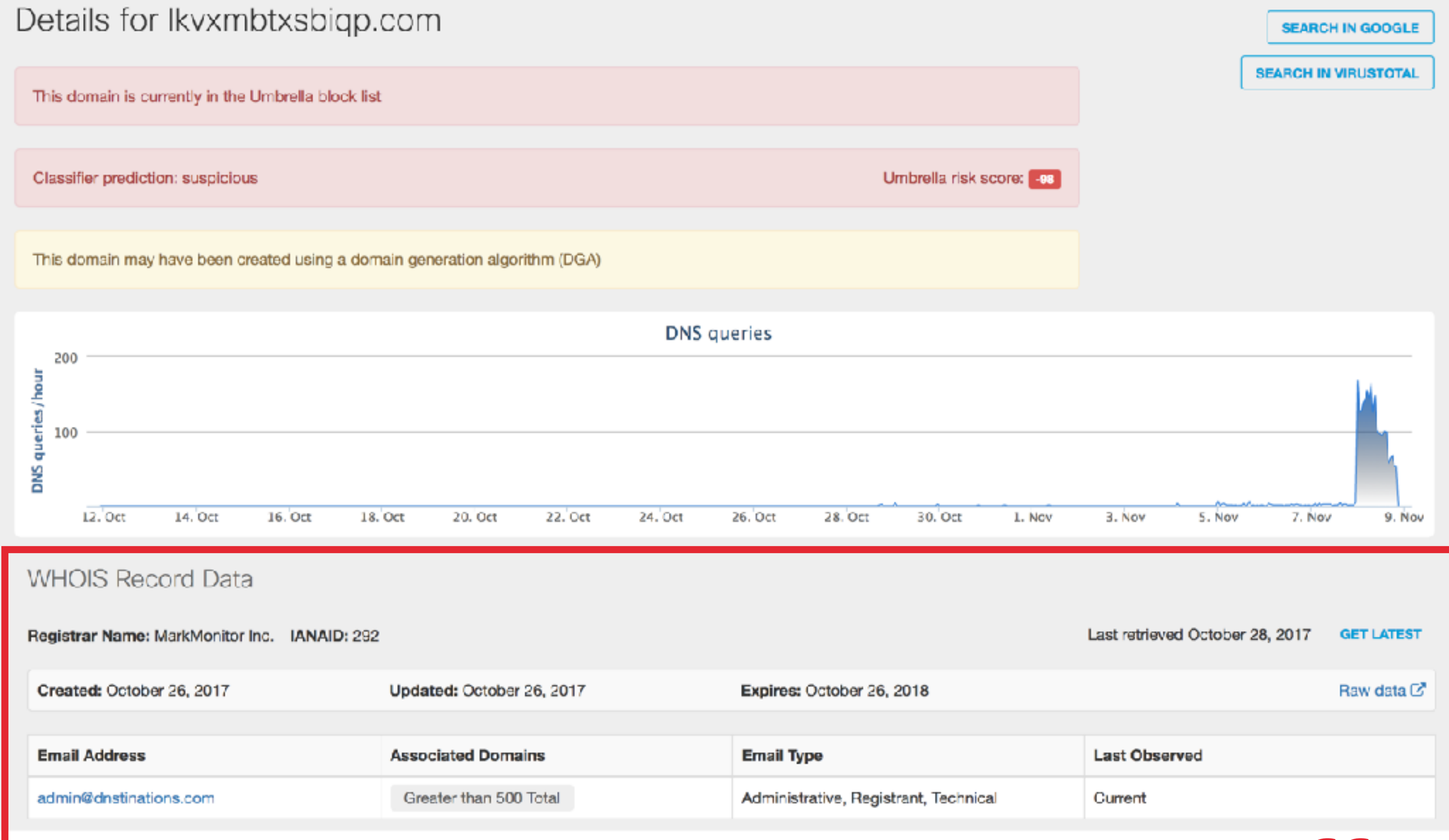
Locky C2:	146.185.249.189
Threat:	C2
Malware:	Locky
URL:	http://146.185.249.189/checkupdate
Host Status:	offline
Firstseen (UTC):	2017-03-02 08:04:55
Lastseen (UTC):	never

Associated IP addresses

The table below shows all ip addresses (e.g. A records) associated with this Locky C2. In case the host is a domain name, the table also shows a history of previous A records if there are any.

Active (?)	Firstseen (UTC)	Lastseen (UTC)	IP address	Hostname	SBL	AS number	AS name	Country
yes	2017-03-02 11:02:00	2017-04-01 05:24:33	146.185.249.189	mail-upnorthdo.permost.net	Not listed	AS44676	VMAGE-AS, RU	Russian Federation (RU)

BEYOND PASSIVE DNS



Details for lkvxmbtxsbiqp.com

This domain is currently in the Umbrella block list

Classifier prediction: suspicious

Umbrella risk score: -98

This domain may have been created using a domain generation algorithm (DGA)

WHOIS Record Data

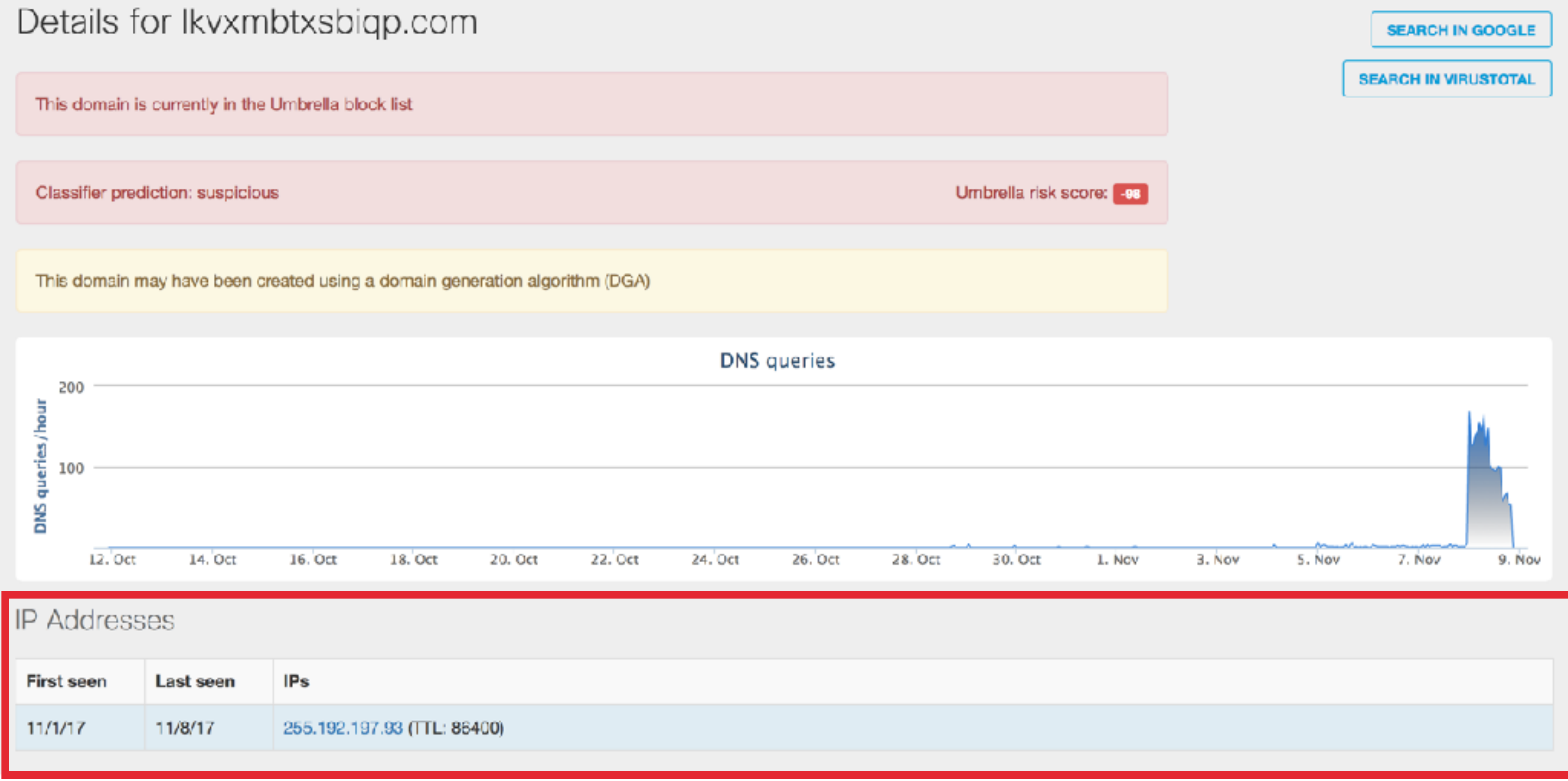
Registrar Name: MarkMonitor Inc. **IANAID:** 292

Last retrieved October 28, 2017

Created: October 26, 2017 **Updated:** October 26, 2017 **Expires:** October 26, 2018

Email Address	Associated Domains	Email Type	Last Observed
admin@dnstinations.com	Greater than 500 Total	Administrative, Registrant, Technical	Current

Additional items to pivot off of: Whois



Details for lkvxmbtxsbiqp.com

This domain is currently in the Umbrella block list

Classifier prediction: suspicious

Umbrella risk score: -98

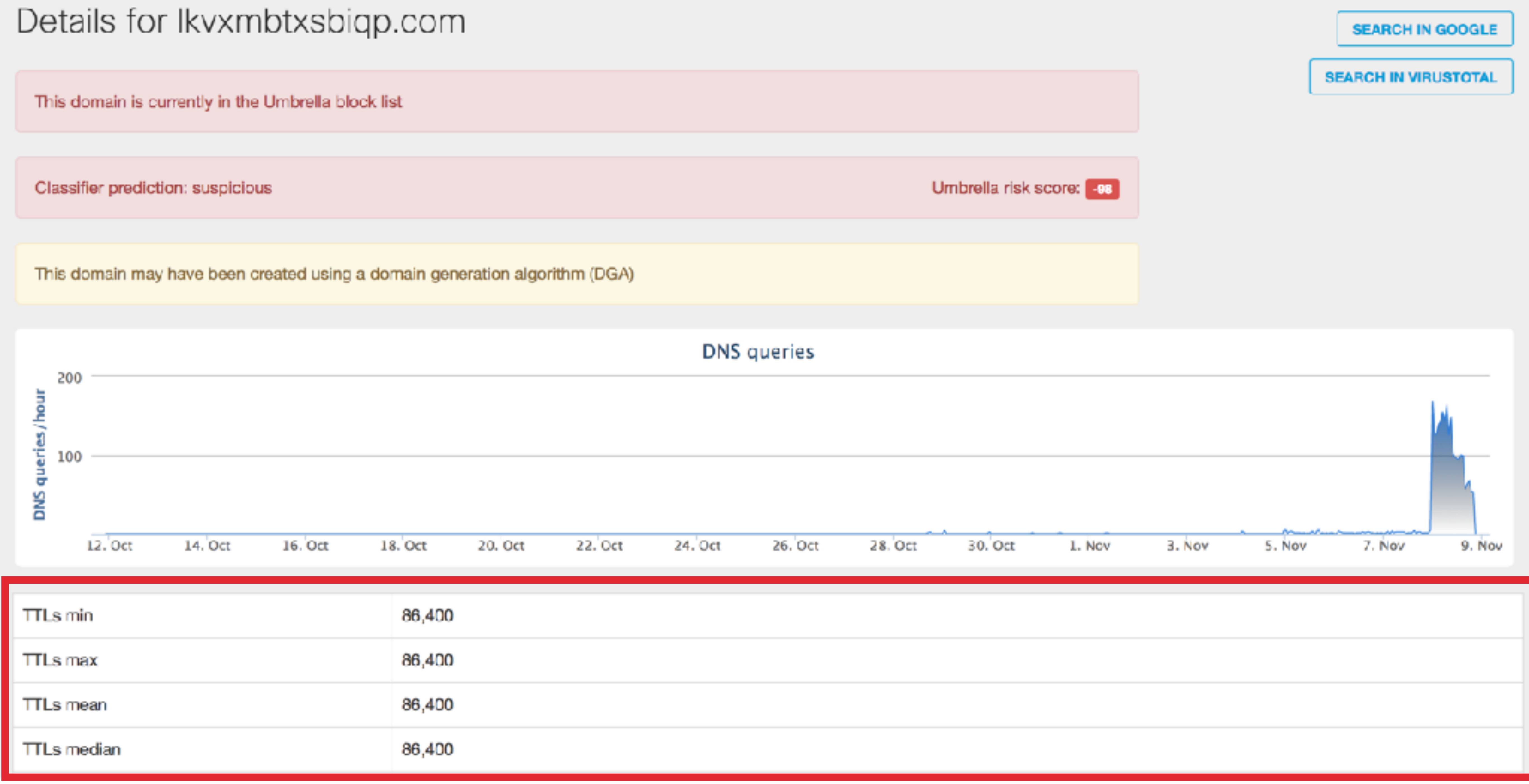
This domain may have been created using a domain generation algorithm (DGA)

IP Addresses

First seen	Last seen	IPs
11/1/17	11/8/17	255.192.197.93 (TTL: 86400)

Additional items to pivot off of: IP’s

DEEPSEC



Details for lkvxmbtxsbiqp.com

This domain is currently in the Umbrella block list

Classifier prediction: suspicious

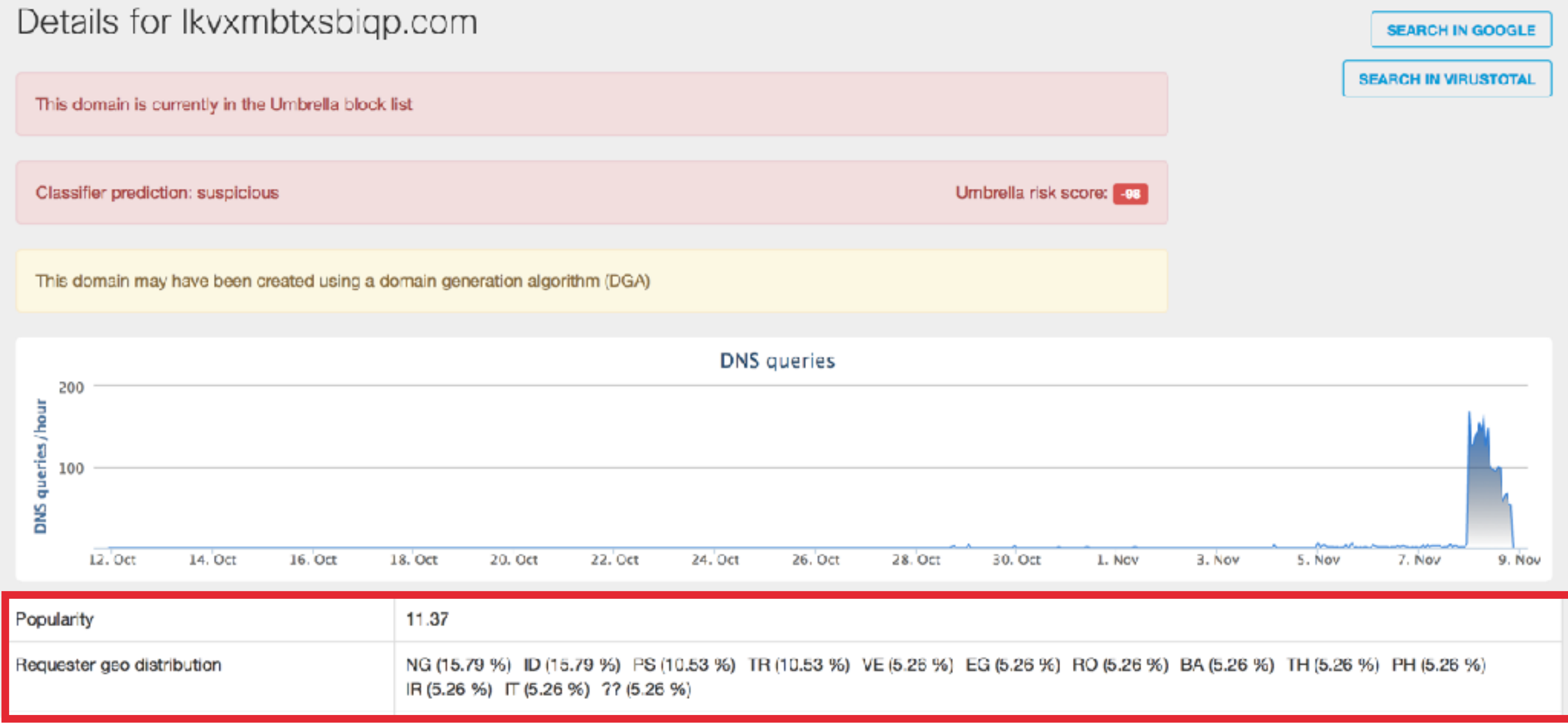
Umbrella risk score: -98

This domain may have been created using a domain generation algorithm (DGA)

TTLs min	86,400
TTLs max	86,400
TTLs mean	86,400
TTLs median	86,400

Additional items to pivot off of: TTL

DEEPSEC



Details for lkvxmbtxsbiqp.com

SEARCH IN GOOGLE

SEARCH IN VIRUSTOTAL

This domain is currently in the Umbrella block list

Classifier prediction: suspicious

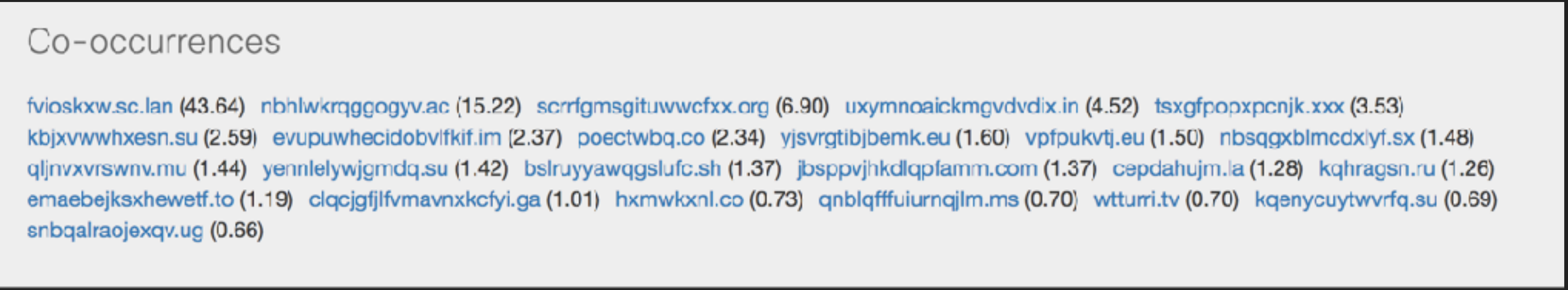
Umbrella risk score: -98

This domain may have been created using a domain generation algorithm (DGA)

Popularity	11.37
Requester geo distribution	NG (15.79 %) ID (15.79 %) PS (10.53 %) TR (10.53 %) VE (5.26 %) EG (5.26 %) RO (5.26 %) BA (5.26 %) TH (5.26 %) PH (5.26 %) IR (5.26 %) IT (5.26 %) ?? (5.26 %)

Additional items to pivot off of: Geo-location of visitors

Additional items to pivot off of: Co-Occurring Domains

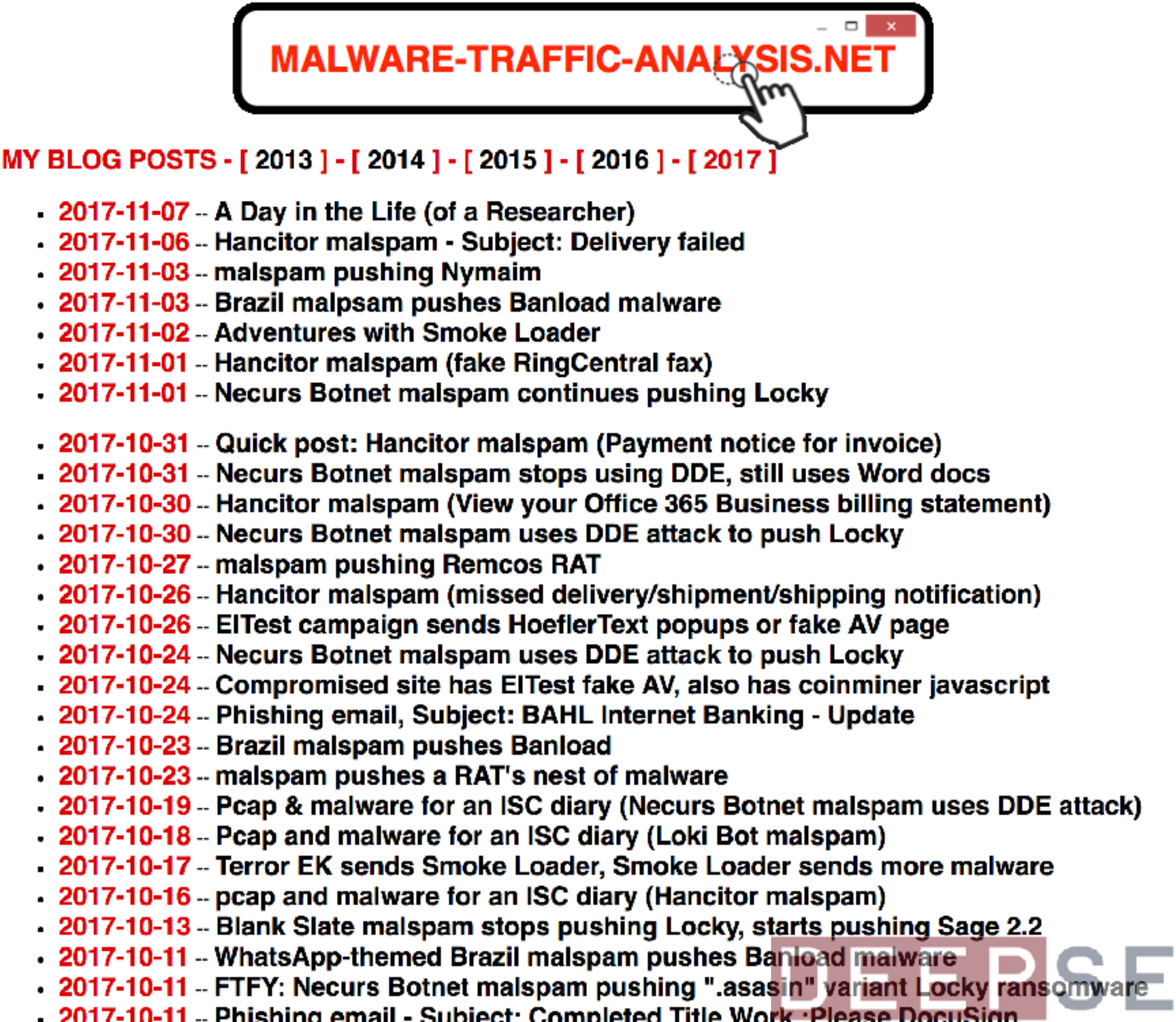


Co-occurrences

fvioskxw.sc.lan (43.64) nbhlwkrqggogyv.ac (15.22) scrrfgmsgituwwcfxx.org (6.90) uxymnoaickmgvdvdix.in (4.52) tsxgfpopxpcnjk.xxx (3.53)
kbjxvwwhxesn.su (2.59) evupuwhecidobvlfkif.im (2.37) poectwbq.co (2.34) yjsvrgtibjbemk.eu (1.60) vpfpukvtj.eu (1.50) nbsqgxblmcdxlyf.sx (1.48)
qljnvxvrswnv.mu (1.44) yennlelywjgmdq.su (1.42) bslruyyawqgslufc.sh (1.37) jbsppvjhkdlqpfamm.com (1.37) cepdahujm.la (1.28) kqhragsn.ru (1.26)
emaebejksxhewetf.to (1.19) clqcjgfjlfvmavnxkcfyi.ga (1.01) hxmwkxnl.co (0.73) qnblqfffuiurnqjlm.ms (0.70) wtturri.tv (0.70) kqenycuytwvrfq.su (0.69)
snbqalraojexqv.ug (0.66)

Finding data using Open Source Intelligence

OSINT



MALWARE-TRAFFIC-ANALYSIS.NET

MY BLOG POSTS - [2013] - [2014] - [2015] - [2016] - [2017]

- 2017-11-07 -- A Day in the Life (of a Researcher)
- 2017-11-06 -- Hancitor malspam - Subject: Delivery failed
- 2017-11-03 -- malspam pushing Nymaim
- 2017-11-03 -- Brazil malpsam pushes Banload malware
- 2017-11-02 -- Adventures with Smoke Loader
- 2017-11-01 -- Hancitor malspam (fake RingCentral fax)
- 2017-11-01 -- Necurs Botnet malspam continues pushing Locky

- 2017-10-31 -- Quick post: Hancitor malspam (Payment notice for invoice)
- 2017-10-31 -- Necurs Botnet malspam stops using DDE, still uses Word docs
- 2017-10-30 -- Hancitor malspam (View your Office 365 Business billing statement)
- 2017-10-30 -- Necurs Botnet malspam uses DDE attack to push Locky
- 2017-10-27 -- malspam pushing Remcos RAT
- 2017-10-26 -- Hancitor malspam (missed delivery/shipment/shipping notification)
- 2017-10-26 -- EITest campaign sends HoeflerText popups or fake AV page
- 2017-10-24 -- Necurs Botnet malspam uses DDE attack to push Locky
- 2017-10-24 -- Compromised site has EITest fake AV, also has coinminer javascript
- 2017-10-24 -- Phishing email, Subject: BAHL Internet Banking - Update
- 2017-10-23 -- Brazil malspam pushes Banload
- 2017-10-23 -- malspam pushes a RAT's nest of malware
- 2017-10-19 -- Pcap & malware for an ISC diary (Necurs Botnet malspam uses DDE attack)
- 2017-10-18 -- Pcap and malware for an ISC diary (Loki Bot malspam)
- 2017-10-17 -- Terror EK sends Smoke Loader, Smoke Loader sends more malware
- 2017-10-16 -- pcap and malware for an ISC diary (Hancitor malspam)
- 2017-10-13 -- Blank Slate malspam stops pushing Locky, starts pushing Sage 2.2
- 2017-10-11 -- WhatsApp-themed Brazil malspam pushes Banload malware
- 2017-10-11 -- FTFY: Necurs Botnet malspam pushing ".asasin" variant Locky ransomware
- 2017-10-11 -- Phishing email - Subject: Completed Title Work :Please DocuSign

My Online Security Keep yourself safe online

Malformed emails from Necurs botnet try to deliver Locky using word docs with embedded OLE objects

7 November 2017 8:21 pm

Double Click Here
To Unlock Contents

Another Locky ransomware campaign that is trying to use Embedded OLE Objects is hitting the UK again (and probably other countries at same time) with an email with a subject of Emailing: JXF53 – 08.11.2017, (random characters and numbers) pretending to come from random senders. Some have a ...

Continue reading →

Malware, Spam embedded OLE object, locky, malware, Ransomware Leave a reply

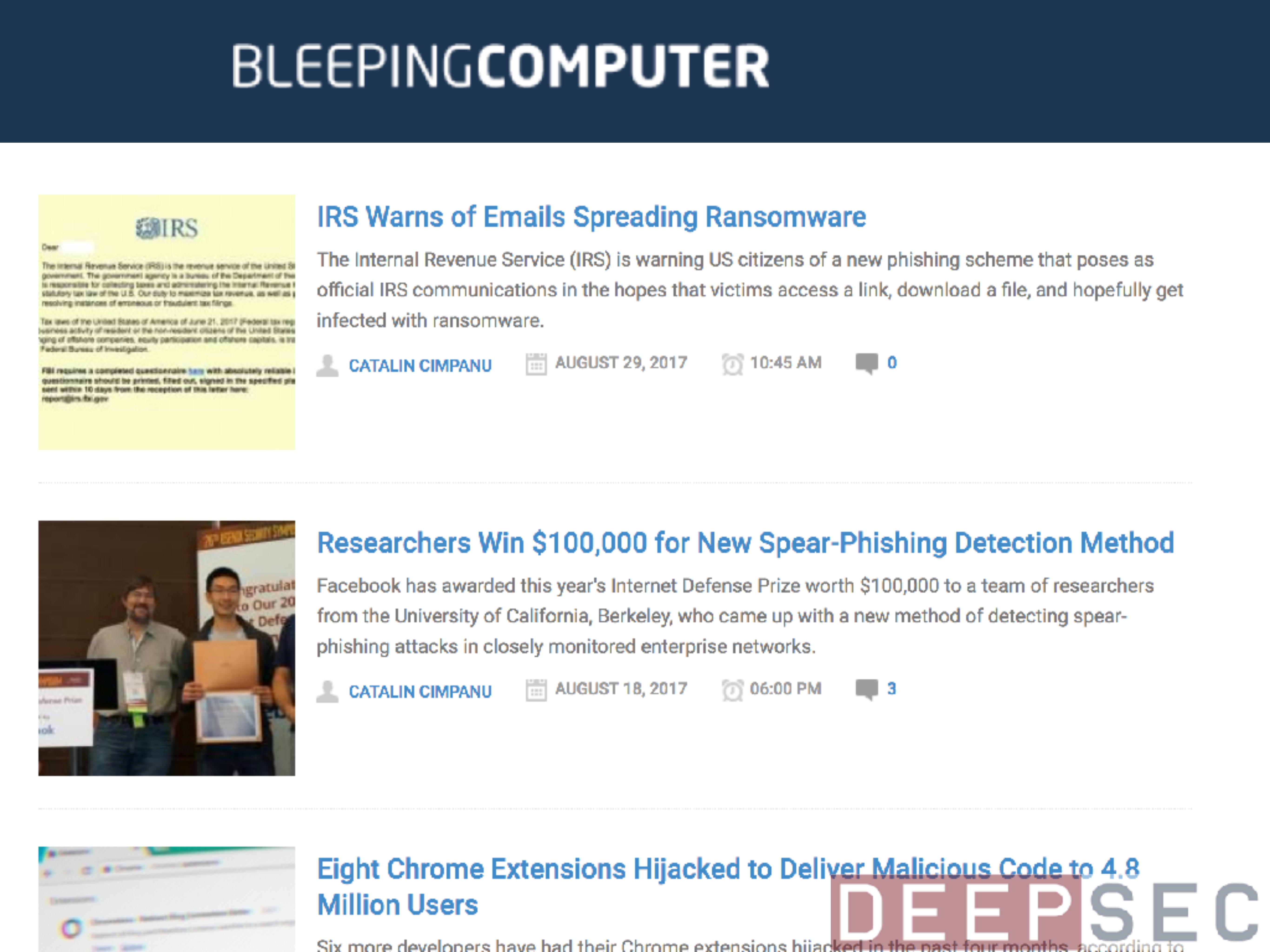
Fake You have a new highly encrypted secure fax from eFax! malspam delivers Trickbot banking Trojan

7 November 2017 11:48 am 1

eFax Corporate

An email with the subject of You have a new fax pretending to come from eFax Corporate but actually coming from a look-a-like domain <message@efax-secure.com> with a malicious word doc attachment is today's latest spoof of a well-known company, bank or public authority delivering Trickbot banking Trojan You can now ...

Continue reading →



BLEEPINGCOMPUTER

IRS

Dear

The Internal Revenue Service (IRS) is the revenue service of the United St
government. The government agency is a bureau of the Department of the
is responsible for collecting taxes and administering the Internal Revenue
statutory tax law of the U.S. Our duty to maximize tax revenue, as well as
resolving instances of erroneous or fraudulent tax filings.

Tax laws of the United States of America of June 21, 2017 (Federal tax reg
business activity of resident or the non-resident citizens of the United States
nging of offshore companies, equity participation and offshore capitals, is tra
Federal Bureau of Investigation.

FBI requires a completed questionnaire here with absolutely reliable
questionnaire should be printed, filled out, signed in the specified pla
sent within 10 days from the reception of this letter here:
report@irs.fbi.gov

IRS Warns of Emails Spreading Ransomware

The Internal Revenue Service (IRS) is warning US citizens of a new phishing scheme that poses as official IRS communications in the hopes that victims access a link, download a file, and hopefully get infected with ransomware.

CATALIN CIMPANU AUGUST 29, 2017 10:45 AM 0

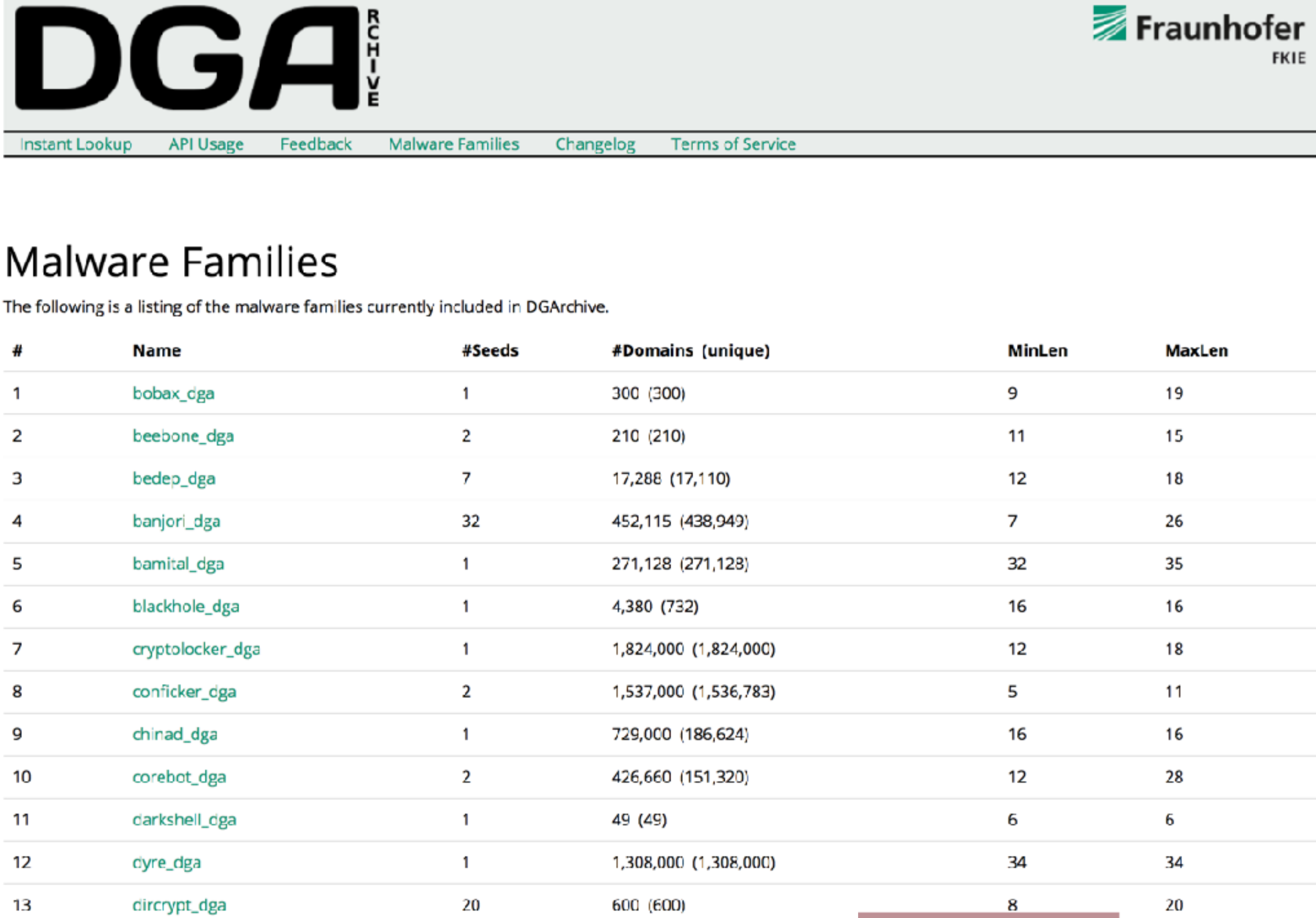
Researchers Win $100,000 for New Spear-Phishing Detection Method

Facebook has awarded this year's Internet Defense Prize worth $100,000 to a team of researchers from the University of California, Berkeley, who came up with a new method of detecting spear-phishing attacks in closely monitored enterprise networks.

CATALIN CIMPANU AUGUST 18, 2017 06:00 PM 3

Eight Chrome Extensions Hijacked to Deliver Malicious Code to 4.8 Million Users

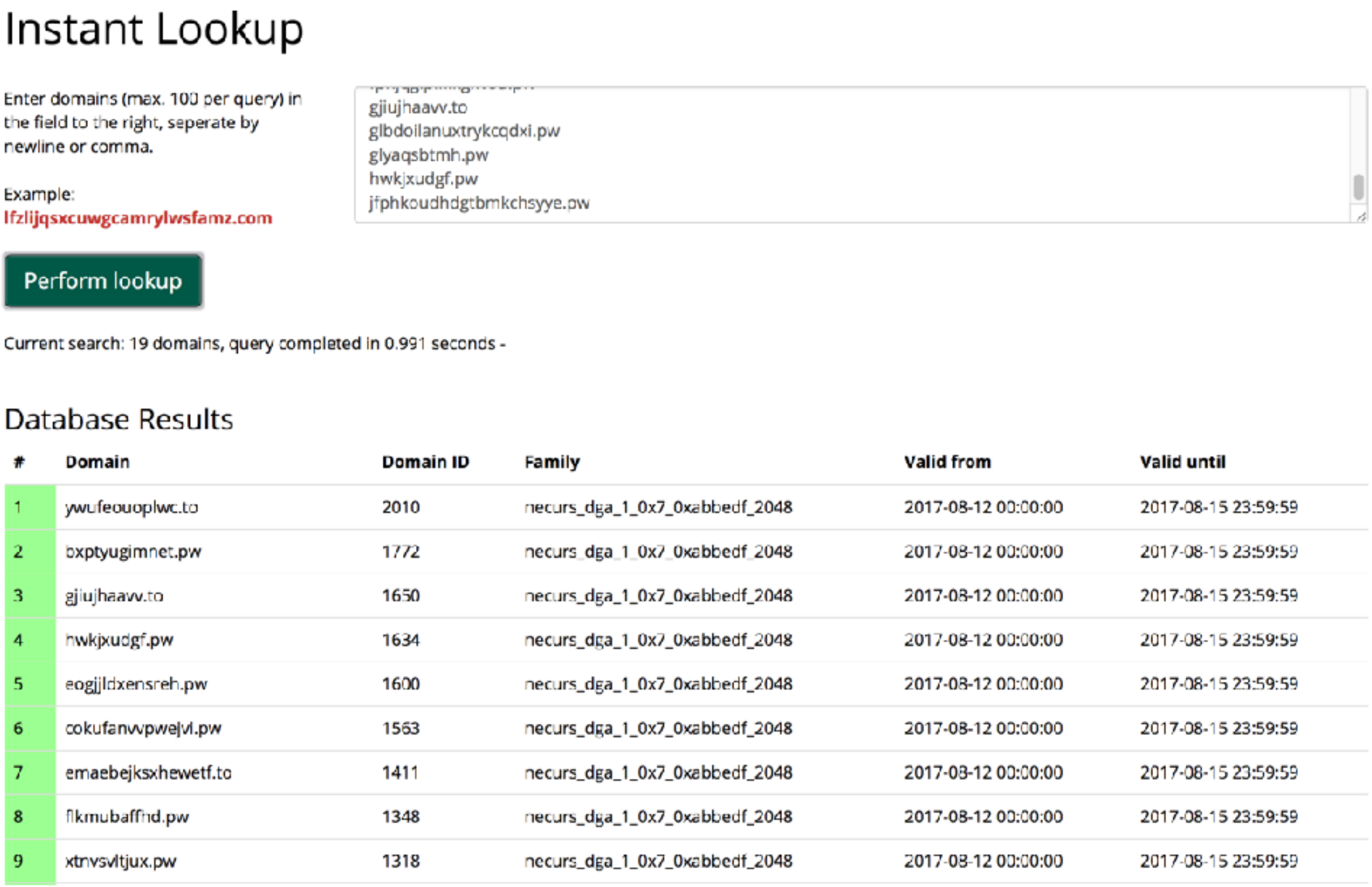
Six more developers have had their Chrome extensions hijacked in the past four months, according to



Malware Families

The following is a listing of the malware families currently included in DGArchive.

#	Name	#Seeds	#Domains (unique)	MinLen	MaxLen
1	bobax_dga	1	300 (300)	9	19
2	beebone_dga	2	210 (210)	11	15
3	bedep_dga	7	17,288 (17,110)	12	18
4	banjori_dga	32	452,115 (438,949)	7	26
5	bamital_dga	1	271,128 (271,128)	32	35
6	blackhole_dga	1	4,380 (732)	16	16
7	cryptolocker_dga	1	1,824,000 (1,824,000)	12	18
8	conficker_dga	2	1,537,000 (1,536,783)	5	11
9	chinad_dga	1	729,000 (186,624)	16	16
10	corebot_dga	2	426,660 (151,320)	12	28
11	darkshell_dga	1	49 (49)	6	6
12	dyre_dga	1	1,308,000 (1,308,000)	34	34
13	dircrypt_dga	20	600 (600)	8	20



Instant Lookup

Enter domains (max. 100 per query) in the field to the right, seperate by newline or comma.

Example:
lfzlijqsxcuwgcamrylwsfamz.com

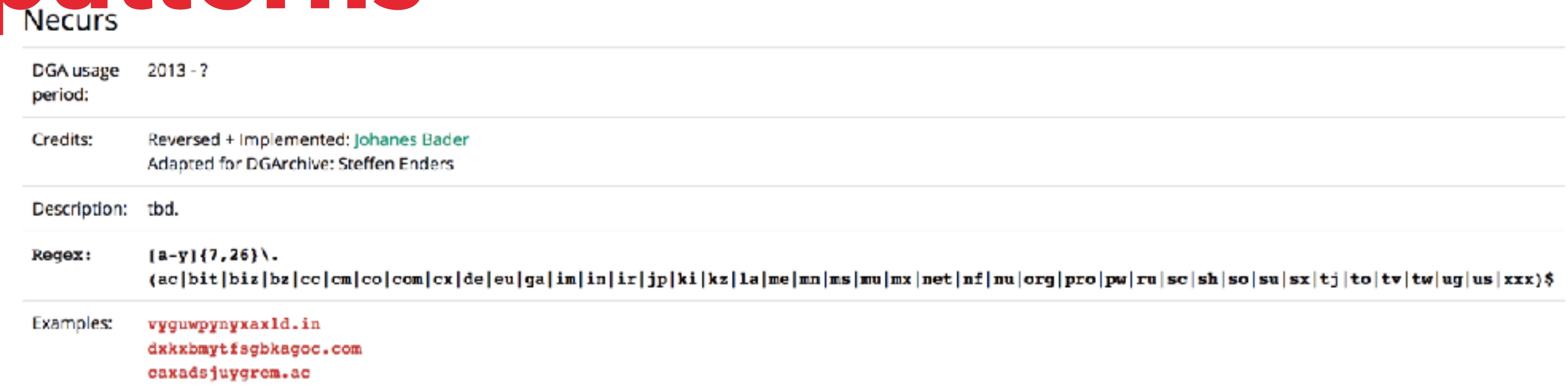
```
gjiujhaavv.to
glbdoilanuxtrykcqdxi.pw
glyaqsbtmh.pw
hwkjxudgf.pw
jfphkoudhdgtbmkchsyye.pw
```

Current search: 19 domains, query completed in 0.991 seconds -

Database Results

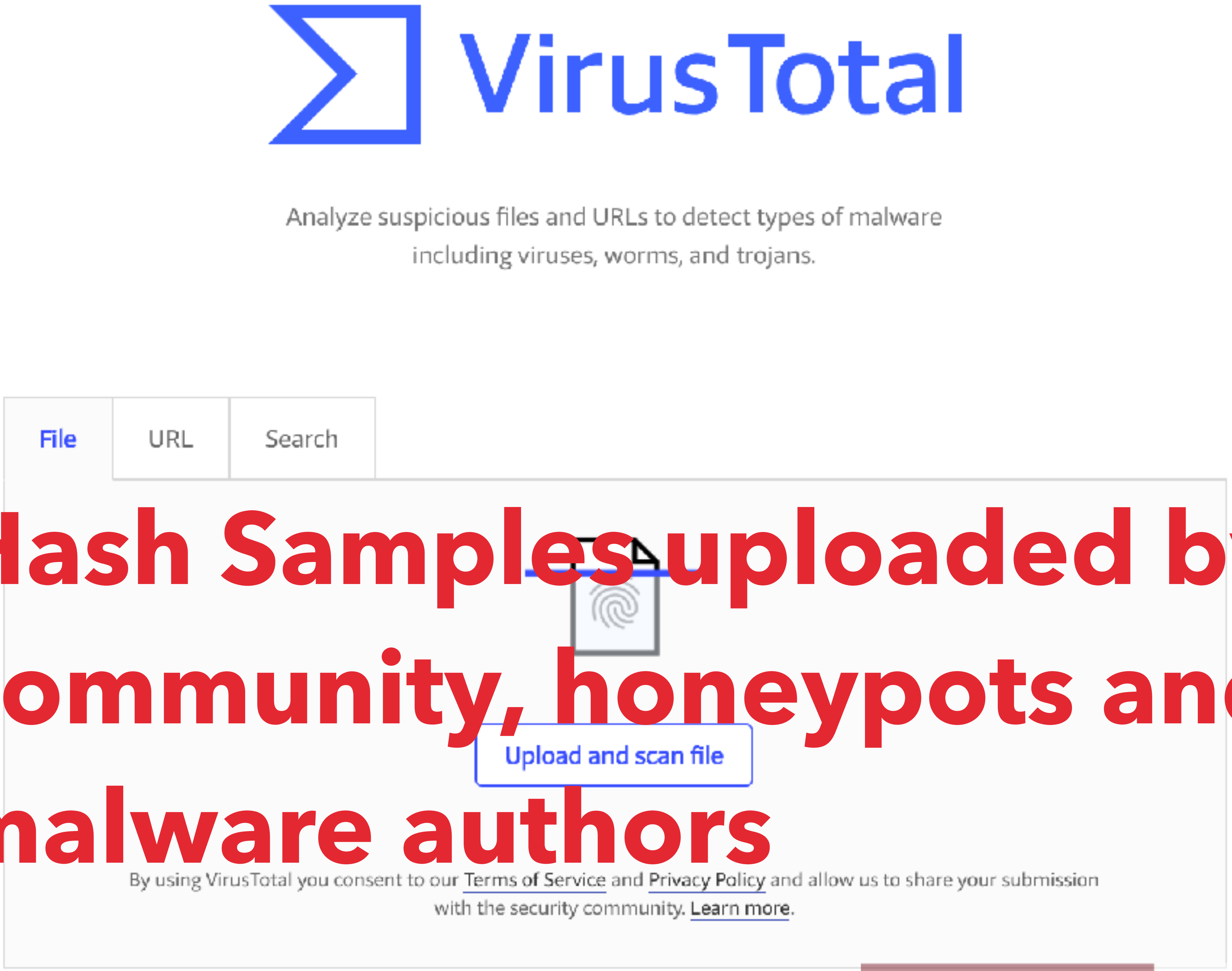
#	Domain	Domain ID	Family	Valid from	Valid until
1	ywufeouoplwc.to	2010	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
2	bxptyugimnet.pw	1772	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
3	gjiujhaavv.to	1650	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
4	hwkjxudgf.pw	1634	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
5	eogjjldxensreh.pw	1600	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
6	cokufanvvpwejvl.pw	1563	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
7	emaebejksxhewetf.to	1411	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
8	flkmubaffhd.pw	1348	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59
9	xtnvsvltjux.pw	1318	necurs_dga_1_0x7_0xabbedf_2048	2017-08-12 00:00:00	2017-08-15 23:59:59

DGA Archive provides regex lookups to find similar patterns



Necurs

DGA usage period:	2013 - ?
Credits:	Reversed + Implemented: Johannes Bader Adapted for DGArchive: Steffen Enders
Description:	tbd.
Regex:	`[a-y]{7,26}\.(ac|bit|biz|bz|cc|cm|co|com|cx|de|eu|ga|im|in|ir|jp|ki|kz|la|me|mn|ms|mu|mx|net|nf|nu|org|pro|pw|ru|sc|sh|so|su|sx|tj|to|tv|tw|ug|us|xxx)$`
Examples:	vyguwpynyxaxld.in dxkxbmytfsgbkagoc.com caxadsjuygrem.ac



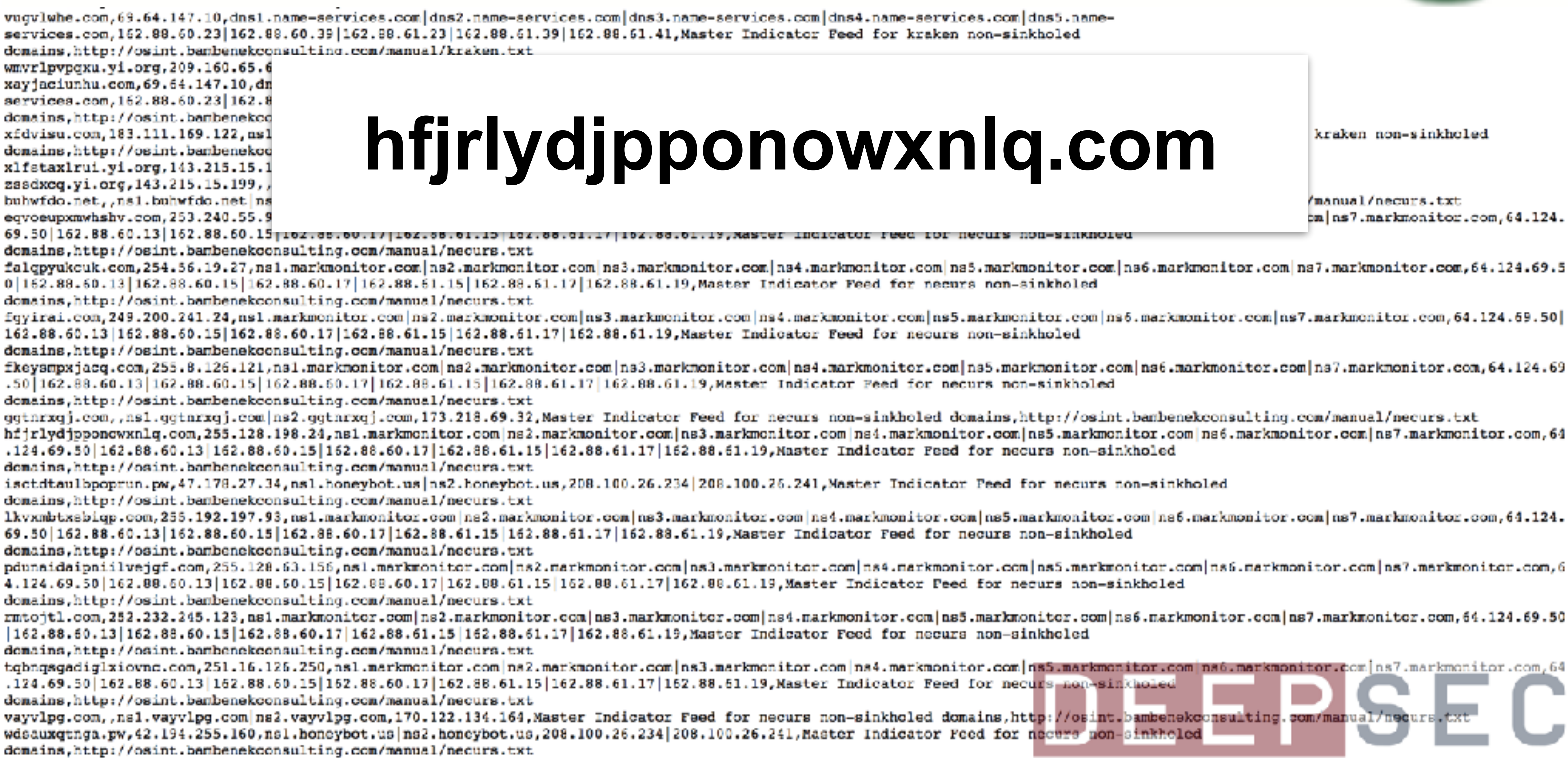
Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

By using VirusTotal you consent to our Terms of Service and Privacy Policy and allow us to share your submission with the security community. Learn more.

Hash Samples uploaded by community, honeypots and malware authors

FEEDS

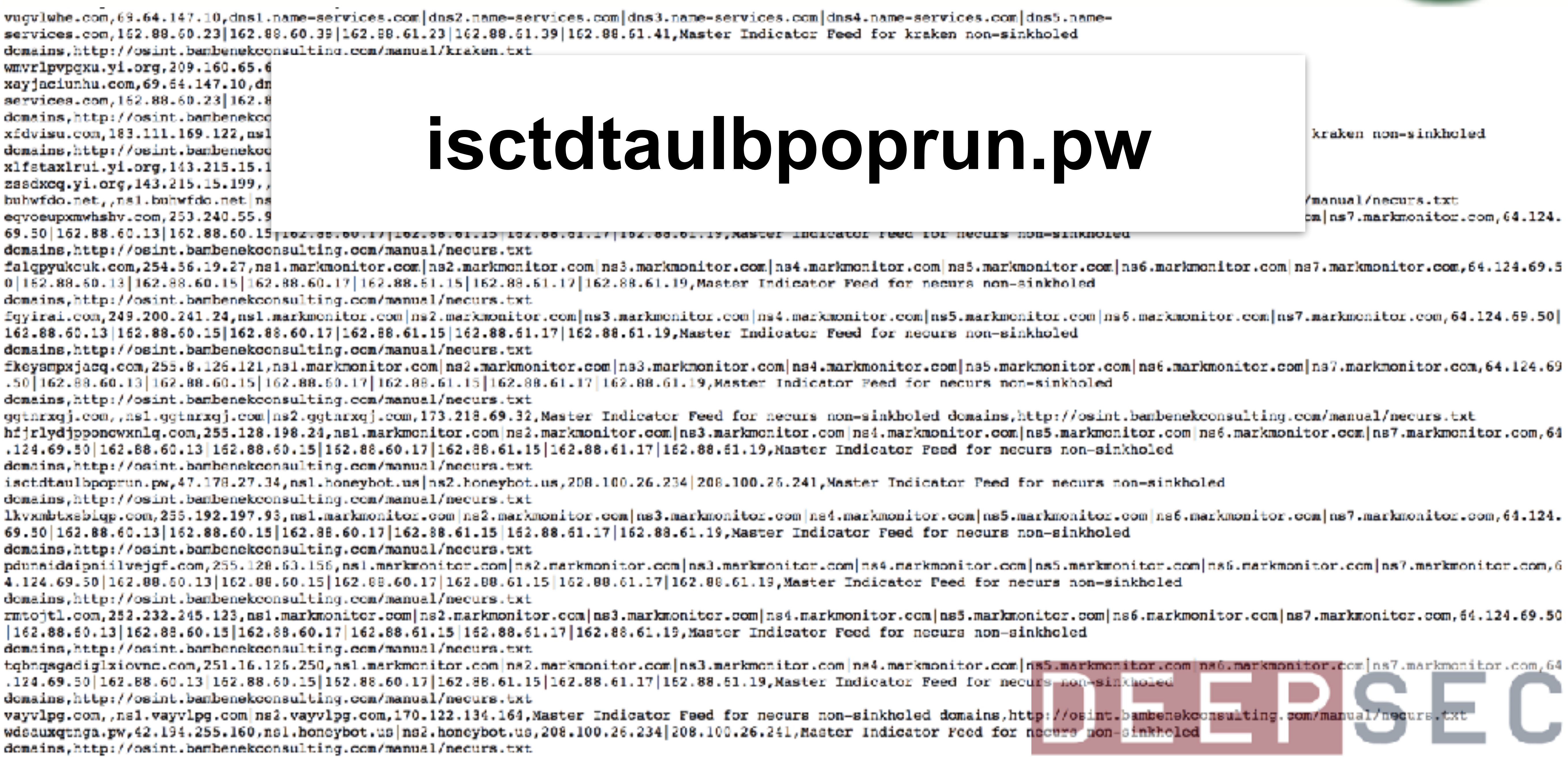
Bambenek Consulting



```
vugvlwhe.com,69.64.147.10,dns1.name-services.com|dns2.name-services.com|dns3.name-services.com|dns4.name-services.com|dns5.name-
services.com,162.88.60.23|162.88.60.39|162.88.61.23|162.88.61.39|162.88.61.41,Master Indicator Feed for kraken non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/kraken.txt
wmvrlpvpqxu.yi.org,209.160.65.6
xayjaciunhu.com,69.64.147.10,dn
services.com,162.88.60.23|162.8
domains,http://osint.bambenekco
xfdvisu.com,183.111.169.122,nsl                                                                                        kraken non-sinkholed
domains,http://osint.bambenekco
xlfstaxlrui.yi.org,143.215.15.1
zssdxcq.yi.org,143.215.15.199,,
buhwfdo.net,,ns1.buhwfdo.net|ns                                                                                  /manual/necurs.txt
eqvoeupxmwhshv.com,253.240.55.9                                                                                  om|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
falqpyukcuk.com,254.56.19.27,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.5
0|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fgyirai.com,249.200.241.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50|
162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fkeysmpxjacq.com,255.8.126.121,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69
.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
ggtnrxqj.com,,ns1.ggtnrxqj.com|ns2.ggtnrxqj.com,173.218.69.32,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
hfjrlydjpponowxnlq.com,255.128.198.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
isctdtaulbpoprun.pw,47.178.27.34,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
lkvxmbtxsblqp.com,255.192.197.93,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
pdunsidaipniilvejgf.com,255.128.63.156,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,6
4.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
rmtojtl.com,252.232.245.123,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50
|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
tqbnqsgadiglxiovnc.com,251.16.126.250,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
vayvlpg.com,,ns1.vayvlpg.com|ns2.vayvlpg.com,170.122.134.164,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
wdsauxqtnga.pw,42.194.255.160,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
```

hfjrlydjpponowxnlq.com

Bambenek Consulting



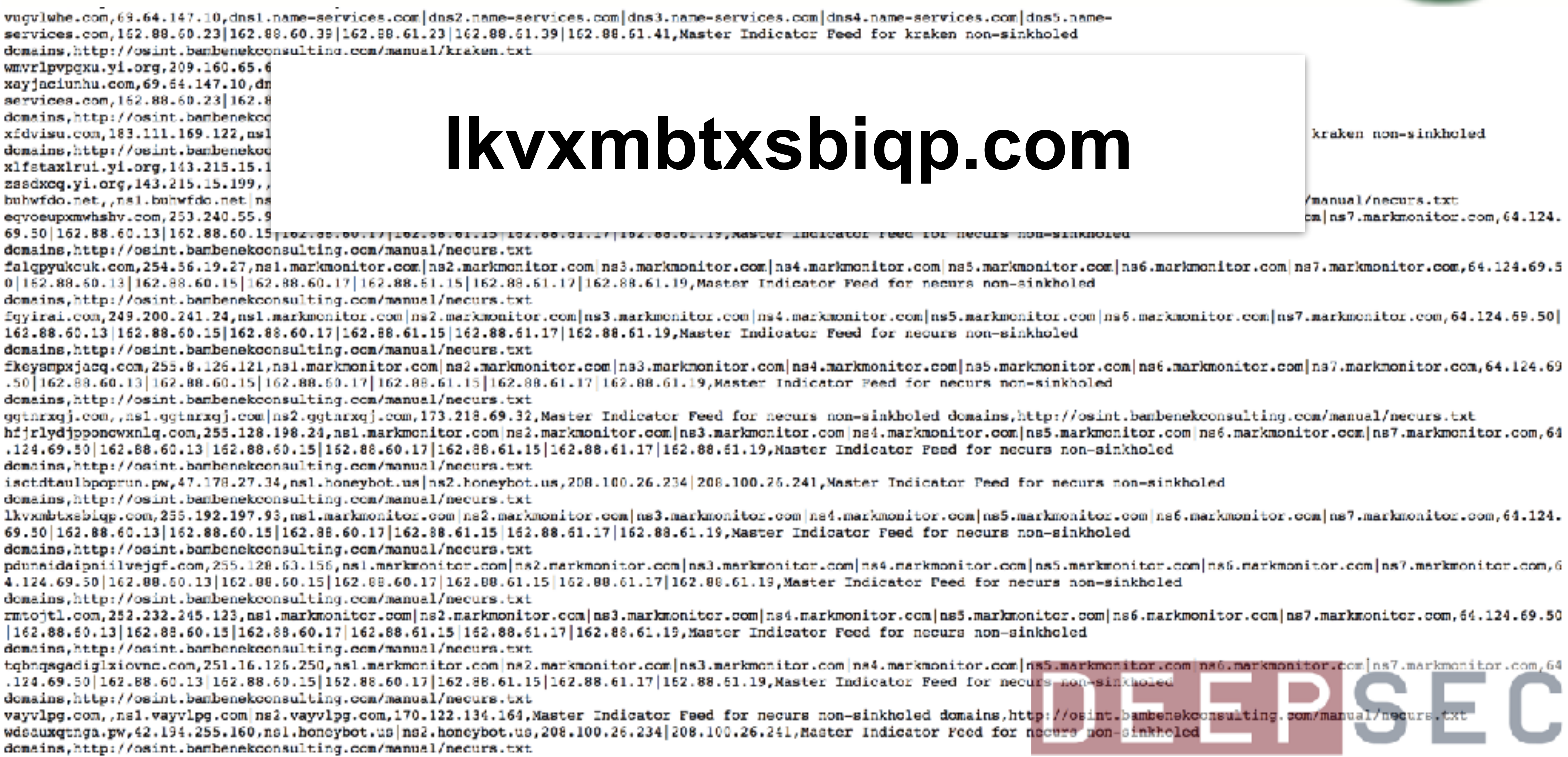
isctdtaulbpoprun.pw

```
vugvlwhe.com,69.64.147.10,dns1.name-services.com|dns2.name-services.com|dns3.name-services.com|dns4.name-services.com|dns5.name-
services.com,162.88.60.23|162.88.60.39|162.88.61.23|162.88.61.39|162.88.61.41,Master Indicator Feed for kraken non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/kraken.txt
wmvrlpvpqxu.yi.org,209.160.65.6
xayjaciunhu.com,69.64.147.10,dn
services.com,162.88.60.23|162.8
domains,http://osint.bambenekco
xfdvisu.com,183.111.169.122,ns1                                                                                      kraken non-sinkholed
domains,http://osint.bambenekco
xlfstaxlrui.yi.org,143.215.15.1
zssdxcq.yi.org,143.215.15.199,,
buhwfdo.net,,ns1.buhwfdo.net|ns                                                                                     /manual/necurs.txt
eqvoeupxmwhshv.com,253.240.55.9                                                                                     om|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
falqpyukcuk.com,254.56.19.27,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.5
0|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fqyirai.com,249.200.241.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50|
162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fkeysmpxjacq.com,255.8.126.121,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69
.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
ggtnrxqj.com,,ns1.ggtnrxqj.com|ns2.ggtnrxqj.com,173.218.69.32,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
hfjrlydjpponcwxnlq.com,255.128.198.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
isctdtaulbpoprun.pw,47.178.27.34,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
lkvxmbtxsblqp.com,255.192.197.93,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
pdunaidaipniilvejgf.com,255.128.63.156,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,6
4.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
rmtojtl.com,252.232.245.123,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50
|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
tqbnqsgadiglxiovnc.com,251.16.126.250,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
vayvlpg.com,,ns1.vayvlpg.com|ns2.vayvlpg.com,170.122.134.164,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
wdsauxqtnga.pw,42.194.255.160,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
```

DEEPSEC

Bambenek Consulting

lkvxmbtxsbiqp.com



```
vugvlwhe.com,69.64.147.10,dns1.name-services.com|dns2.name-services.com|dns3.name-services.com|dns4.name-services.com|dns5.name-
services.com,162.88.60.23|162.88.60.39|162.88.61.23|162.88.61.39|162.88.61.41,Master Indicator Feed for kraken non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/kraken.txt
wmvrlpvpqxu.yi.org,209.160.65.6
xayjaciunhu.com,69.64.147.10,dn
services.com,162.88.60.23|162.8
domains,http://osint.bambenekco
xfdvisu.com,183.111.169.122,nsl                                                                          kraken non-sinkholed
domains,http://osint.bambenekco
xlfstaxlrui.yi.org,143.215.15.1
zssdxcq.yi.org,143.215.15.199,,
buhwfdo.net,,ns1.buhwfdo.net|ns                                                                          /manual/necurs.txt
eqvoeupxmwhshv.com,253.240.55.9                                                                          om|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
falqpyukcuk.com,254.56.19.27,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.5
0|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fgyirai.com,249.200.241.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50|
162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
fkeysmpxjacq.com,255.8.126.121,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69
.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
ggtnrxqj.com,,ns1.ggtnrxqj.com|ns2.ggtnrxqj.com,173.218.69.32,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
hfjrlydjpponcwxnlq.com,255.128.198.24,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
isctdtaulbpoprun.pw,47.178.27.34,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
lkvxmbtxsbiqp.com,255.192.197.93,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.
69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
pdunaidaipniilvejgf.com,255.128.63.156,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,6
4.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
rmtojtl.com,252.232.245.123,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64.124.69.50
|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
tqbnqsgadiglxiovnc.com,251.16.126.250,ns1.markmonitor.com|ns2.markmonitor.com|ns3.markmonitor.com|ns4.markmonitor.com|ns5.markmonitor.com|ns6.markmonitor.com|ns7.markmonitor.com,64
.124.69.50|162.88.60.13|162.88.60.15|162.88.60.17|162.88.61.15|162.88.61.17|162.88.61.19,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
vayvlpg.com,,ns1.vayvlpg.com|ns2.vayvlpg.com,170.122.134.164,Master Indicator Feed for necurs non-sinkholed domains,http://osint.bambenekconsulting.com/manual/necurs.txt
wdsauxqtnga.pw,42.194.255.160,ns1.honeybot.us|ns2.honeybot.us,208.100.26.234|208.100.26.241,Master Indicator Feed for necurs non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/necurs.txt
```

DEEPSEC

UNCOVERING INFRASTRUCTURE

IOCS

IOCs SEEN THROUGHOUT THE BOT LIFECYCLE

- DOMAIN NAMES
  - C&C communications
  - DGAs - resolving and NX domains

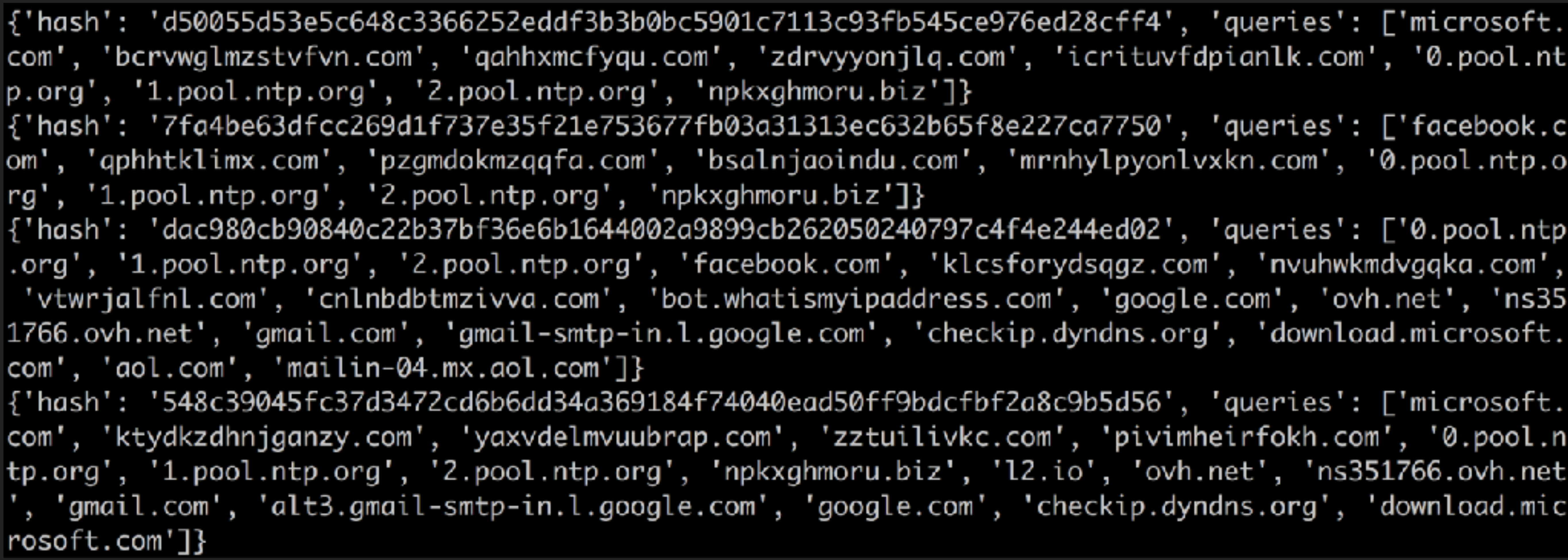
- IP ADDRESSES
  - Hosting IPs

- NAMSERVERS, EMAIL REGISTRANT
  - WHOIS Information

- HASHES OF MALICIOUS BINARIES
  - Dropped by RATS
  - Contained in Spam
  - Dropped by compromised websites or malvertising

CLEANING THE DATA

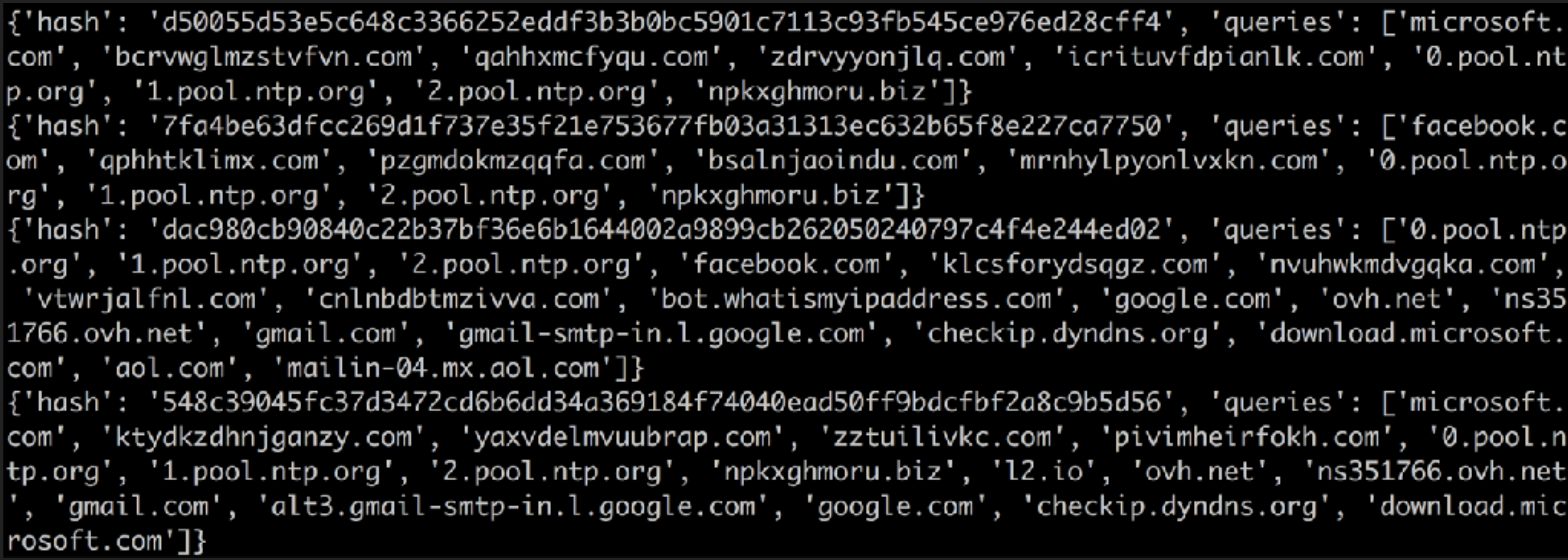
Process data and organize



```
{'hash': 'd50055d53e5c648c3366252eddf3b3b0bc5901c7113c93fb545ce976ed28cff4', 'queries': ['microsoft.
com', 'bcrvwglmzstvfvn.com', 'qahhxmcfyqu.com', 'zdrvyyonjlq.com', 'icrituvfdpianlk.com', '0.pool.nt
p.org', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz']}
{'hash': '7fa4be63dfcc269d1f737e35f21e753677fb03a31313ec632b65f8e227ca7750', 'queries': ['facebook.c
om', 'qphhtklimx.com', 'pzgmdokmzqqfa.com', 'bsalnjaoindu.com', 'mrnhylpyonlvxkn.com', '0.pool.ntp.o
rg', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz']}
{'hash': 'dac980cb90840c22b37bf36e6b1644002a9899cb262050240797c4f4e244ed02', 'queries': ['0.pool.ntp
.org', '1.pool.ntp.org', '2.pool.ntp.org', 'facebook.com', 'klcsforydsqgz.com', 'nvuhwkmdvgqka.com',
 'vtwrjalfnl.com', 'cnlnbdbtmzivva.com', 'bot.whatismyipaddress.com', 'google.com', 'ovh.net', 'ns35
1766.ovh.net', 'gmail.com', 'gmail-smtp-in.l.google.com', 'checkip.dyndns.org', 'download.microsoft.
com', 'aol.com', 'mailin-04.mx.aol.com']}
{'hash': '548c39045fc37d3472cd6b6dd34a369184f74040ead50ff9bdcfbf2a8c9b5d56', 'queries': ['microsoft.
com', 'ktydkzdhnjganzy.com', 'yaxvdelmvuubrap.com', 'zztuilivkc.com', 'pivimheirfokh.com', '0.pool.n
tp.org', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz', 'l2.io', 'ovh.net', 'ns351766.ovh.net
', 'gmail.com', 'alt3.gmail-smtp-in.l.google.com', 'google.com', 'checkip.dyndns.org', 'download.mic
rosoft.com']}
```

Process data and organize

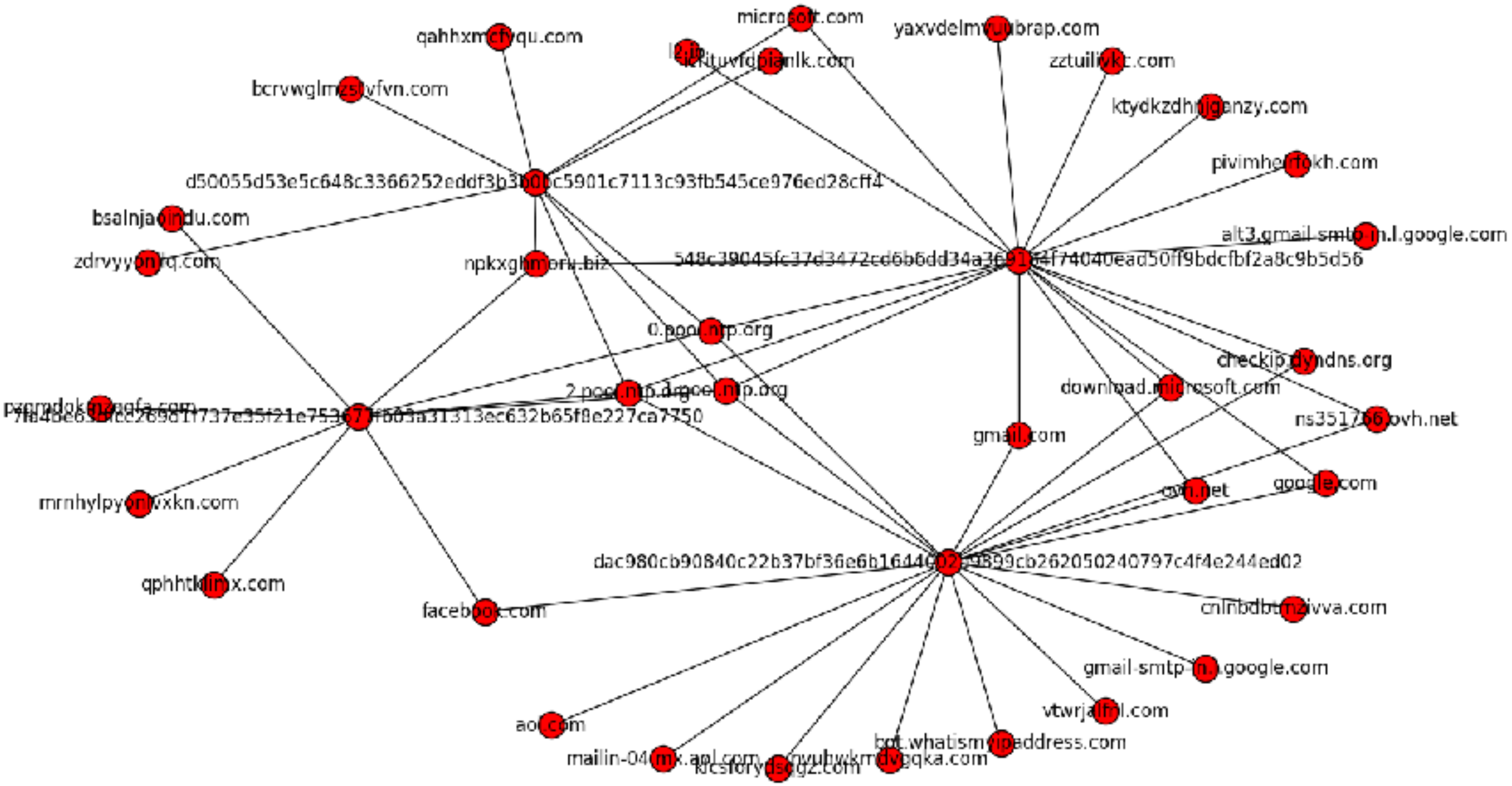
Still A Pain



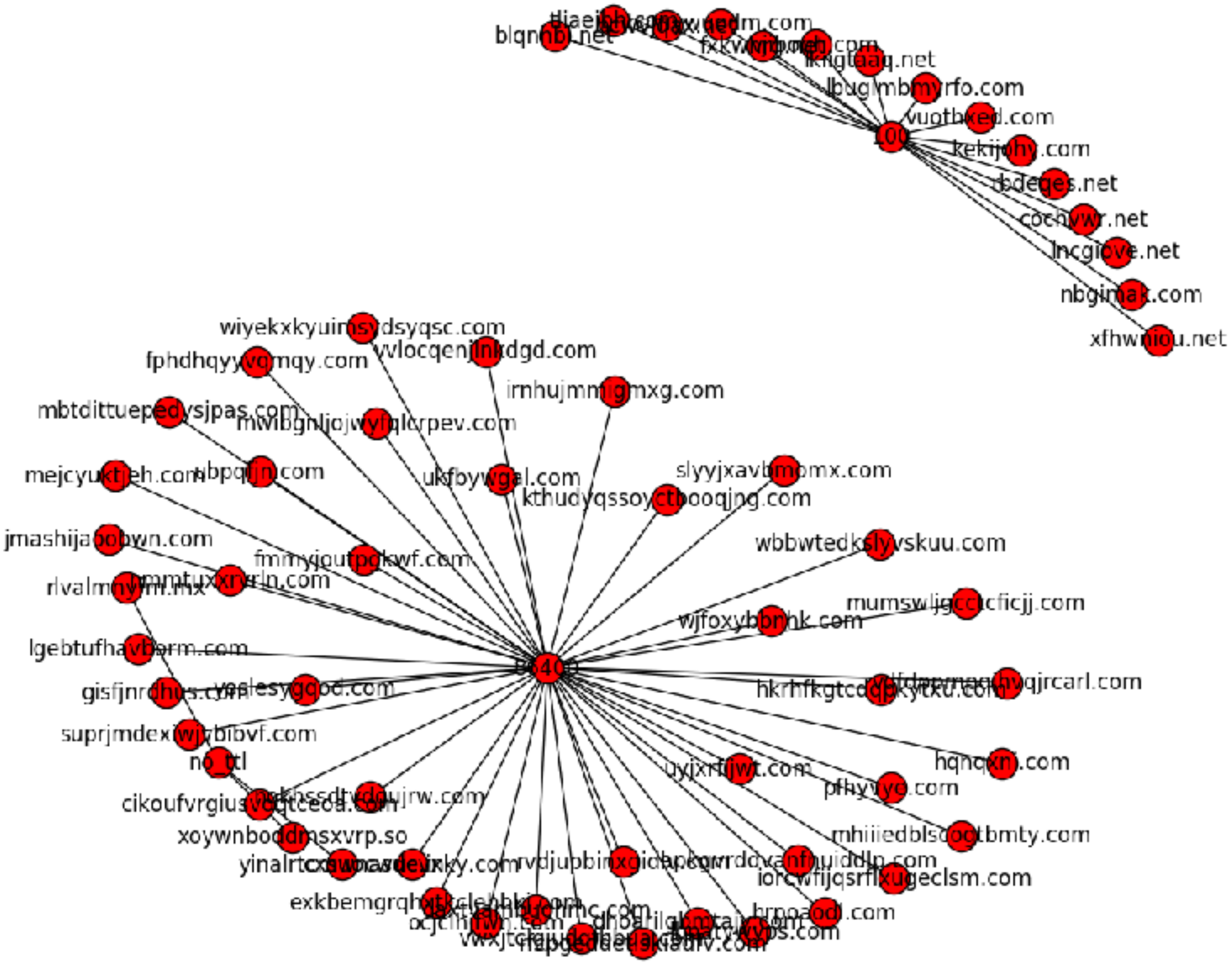
```
{'hash': 'd50055d53e5c648c3366252eddf3b3b0bc5901c7113c93fb545ce976ed28cff4', 'queries': ['microsoft.
com', 'bcrvwglmzstvfvn.com', 'qahhxmcfyqu.com', 'zdrvyyonjlq.com', 'icrituvfdpianlk.com', '0.pool.nt
p.org', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz']}
{'hash': '7fa4be63dfcc269d1f737e35f21e753677fb03a31313ec632b65f8e227ca7750', 'queries': ['facebook.c
om', 'qphhtklimx.com', 'pzgmdokmzqqfa.com', 'bsalnjaoindu.com', 'mrnhylpyonlvxkn.com', '0.pool.ntp.o
rg', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz']}
{'hash': 'dac980cb90840c22b37bf36e6b1644002a9899cb262050240797c4f4e244ed02', 'queries': ['0.pool.ntp
.org', '1.pool.ntp.org', '2.pool.ntp.org', 'facebook.com', 'klcsforydsqgz.com', 'nvuhwkmdvgqka.com',
 'vtwrjalfnl.com', 'cnlnbdbtmzivva.com', 'bot.whatismyipaddress.com', 'google.com', 'ovh.net', 'ns35
1766.ovh.net', 'gmail.com', 'gmail-smtp-in.l.google.com', 'checkip.dyndns.org', 'download.microsoft.
com', 'aol.com', 'mailin-04.mx.aol.com']}
{'hash': '548c39045fc37d3472cd6b6dd34a369184f74040ead50ff9bdcfbf2a8c9b5d56', 'queries': ['microsoft.
com', 'ktydkzdhnjganzy.com', 'yaxvdelmvuubrap.com', 'zztuilivkc.com', 'pivimheirfokh.com', '0.pool.n
tp.org', '1.pool.ntp.org', '2.pool.ntp.org', 'npkxghmoru.biz', 'l2.io', 'ovh.net', 'ns351766.ovh.net
', 'gmail.com', 'alt3.gmail-smtp-in.l.google.com', 'google.com', 'checkip.dyndns.org', 'download.mic
rosoft.com']}
```

To Look At

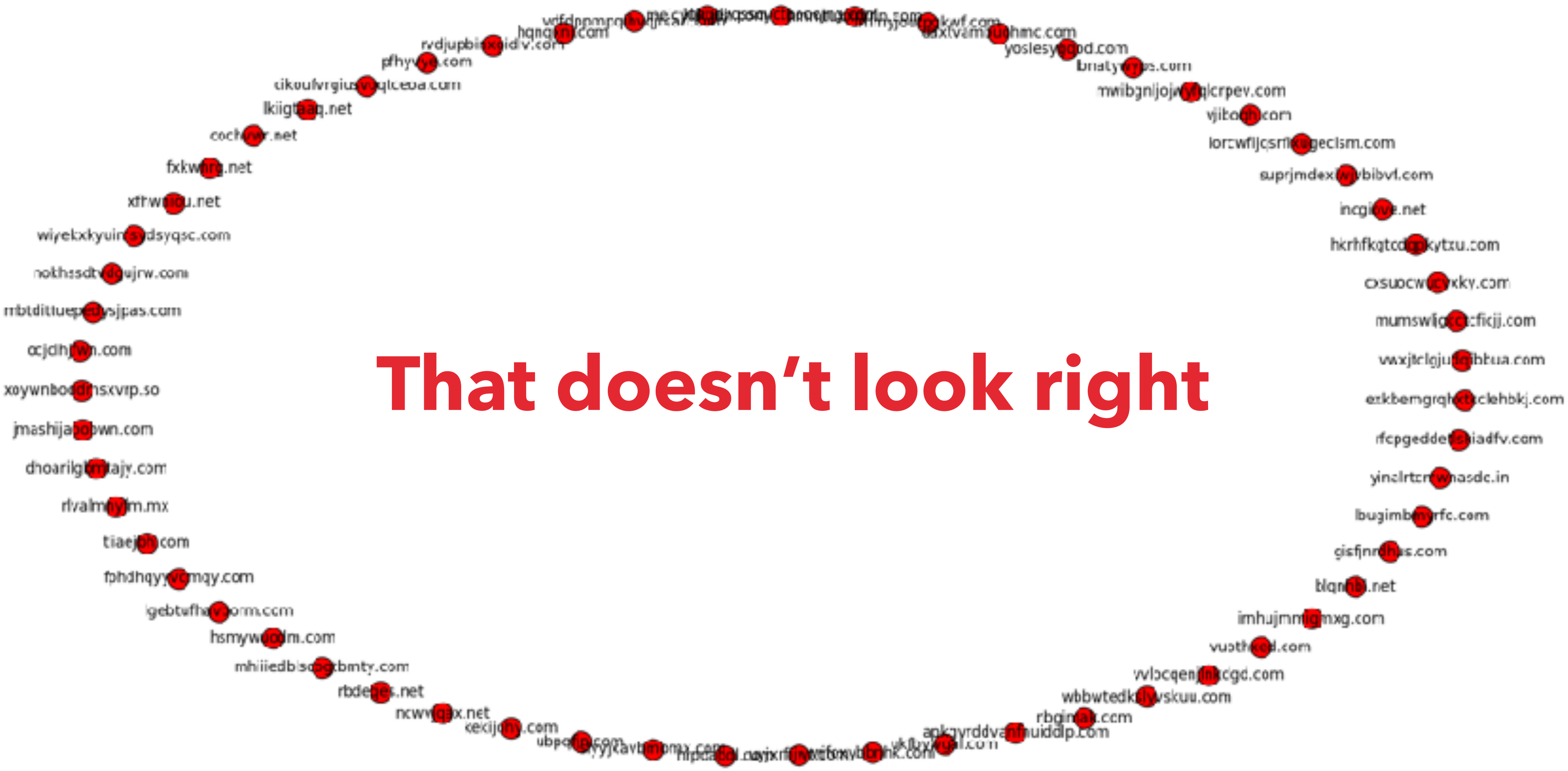
Visually map hash to domain



Visually map TTL to domain

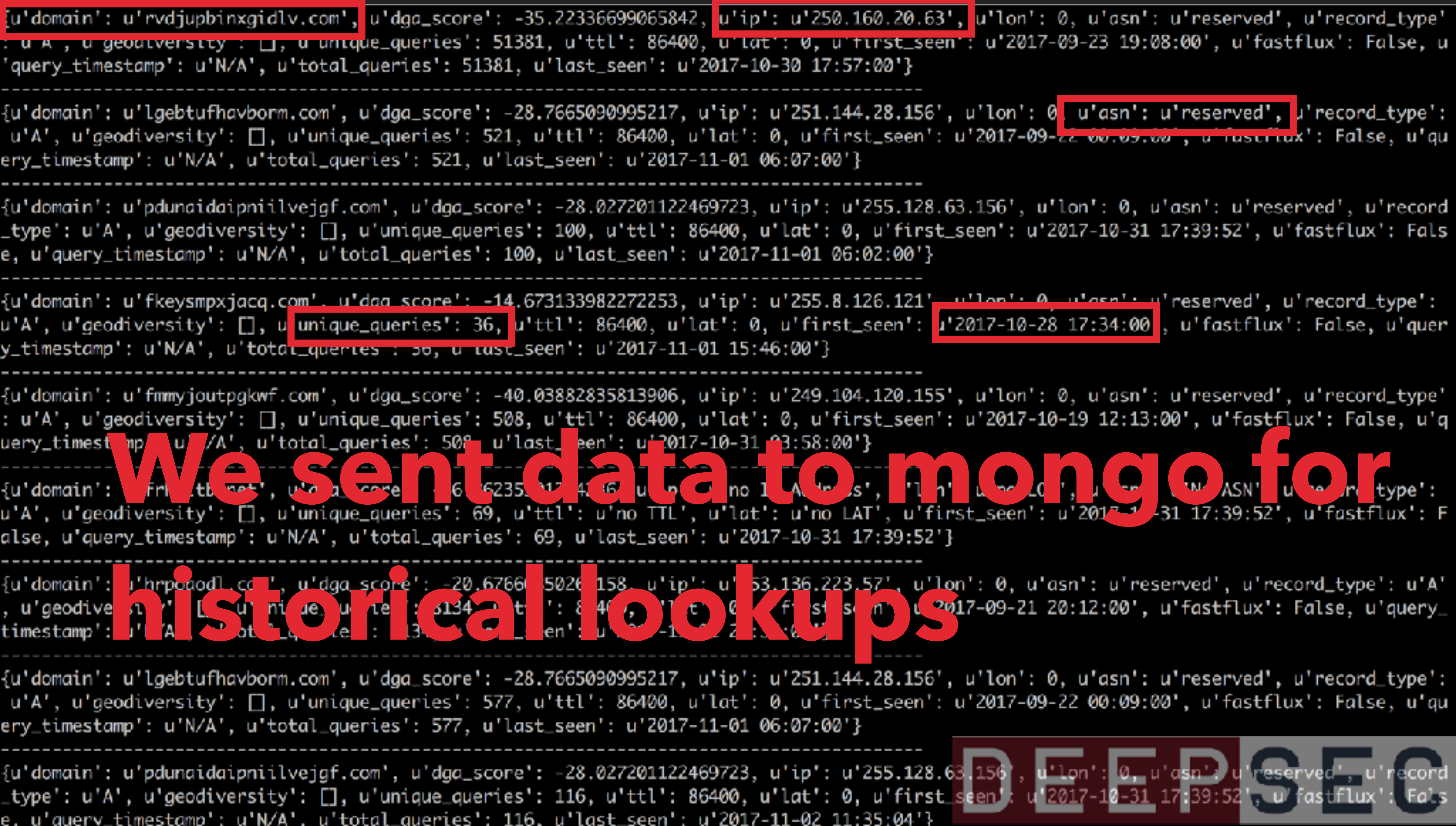


Clean data for useful visuals



That doesn't look right

MONGO DB



```
{u'domain': u'rvdjupbinxgidlv.com', u'dga_score': -35.22336699065842, u'ip': u'250.160.20.63', u'lon': 0, u'asn': u'reserved', u'record_type'
: u'A', u'geodiversity': [], u'unique_queries': 51381, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-09-23 19:08:00', u'fastflux': False, u
'query_timestamp': u'N/A', u'total_queries': 51381, u'last_seen': u'2017-10-30 17:57:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'lgebtufhavborm.com', u'dga_score': -28.7665090995217, u'ip': u'251.144.28.156', u'lon': 0, u'asn': u'reserved', u'record_type':
 u'A', u'geodiversity': [], u'unique_queries': 521, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-09-22 00:09:00', u'fastflux': False, u'qu
ery_timestamp': u'N/A', u'total_queries': 521, u'last_seen': u'2017-11-01 06:07:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'pdunaidaipniilvejgf.com', u'dga_score': -28.027201122469723, u'ip': u'255.128.63.156', u'lon': 0, u'asn': u'reserved', u'record
_type': u'A', u'geodiversity': [], u'unique_queries': 100, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-10-31 17:39:52', u'fastflux': Fals
e, u'query_timestamp': u'N/A', u'total_queries': 100, u'last_seen': u'2017-11-01 06:02:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'fkeysmpxjacq.com', u'dga_score': -14.673133982272253, u'ip': u'255.8.126.121', u'lon': 0, u'asn': u'reserved', u'record_type':
u'A', u'geodiversity': [], u'unique_queries': 36, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-10-28 17:34:00', u'fastflux': False, u'quer
y_timestamp': u'N/A', u'total_queries': 36, u'last_seen': u'2017-11-01 15:46:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'fmmyjoutpgkwf.com', u'dga_score': -40.03882835813906, u'ip': u'249.104.120.155', u'lon': 0, u'asn': u'reserved', u'record_type'
: u'A', u'geodiversity': [], u'unique_queries': 508, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-10-19 12:13:00', u'fastflux': False, u'q
uery_timestamp': u'N/A', u'total_queries': 508, u'last_seen': u'2017-10-31 03:58:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'fr[illegible]tb.net', u'dga_score': -16.6235[illegible], u'ip': u'no IP Address', u'lon': u'no LON', u'asn': u'NO ASN', u'record_type':
u'A', u'geodiversity': [], u'unique_queries': 69, u'ttl': u'no TTL', u'lat': u'no LAT', u'first_seen': u'2017-10-31 17:39:52', u'fastflux': F
alse, u'query_timestamp': u'N/A', u'total_queries': 69, u'last_seen': u'2017-10-31 17:39:52'}
------------------------------------------------------------------------------------------------
{u'domain': u'hrpdaodl.com', u'dga_score': -20.6766[illegible]5026158, u'ip': u'[illegible]53.136.223.57', u'lon': 0, u'asn': u'reserved', u'record_type': u'A'
, u'geodiversity': [], u'unique_queries': [illegible]134, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-09-21 20:12:00', u'fastflux': False, u'query_
timestamp': u'N/A', u'total_queries': 13[illegible], u'last_seen': u'2017-1[illegible]'}
------------------------------------------------------------------------------------------------
{u'domain': u'lgebtufhavborm.com', u'dga_score': -28.7665090995217, u'ip': u'251.144.28.156', u'lon': 0, u'asn': u'reserved', u'record_type':
 u'A', u'geodiversity': [], u'unique_queries': 577, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-09-22 00:09:00', u'fastflux': False, u'qu
ery_timestamp': u'N/A', u'total_queries': 577, u'last_seen': u'2017-11-01 06:07:00'}
------------------------------------------------------------------------------------------------
{u'domain': u'pdunaidaipniilvejgf.com', u'dga_score': -28.027201122469723, u'ip': u'255.128.63.156', u'lon': 0, u'asn': u'reserved', u'record
_type': u'A', u'geodiversity': [], u'unique_queries': 116, u'ttl': 86400, u'lat': 0, u'first_seen': u'2017-10-31 17:39:52', u'fastflux': Fals
e, u'query_timestamp': u'N/A', u'total_queries': 116, u'last_seen': u'2017-11-02 11:35:04'}
```

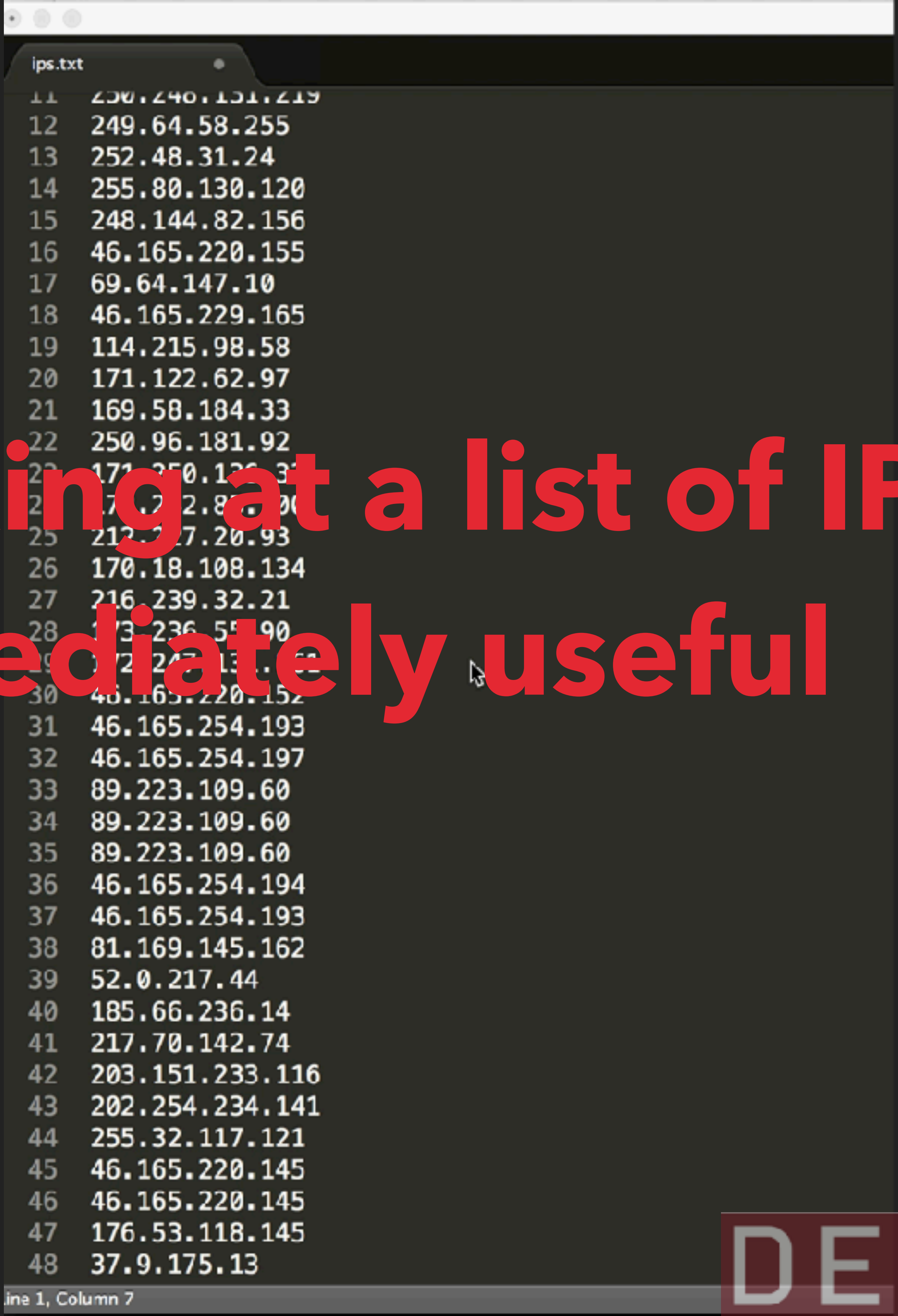
We sent data to mongo for historical lookups

CLEANING DATA

- 175 IPs related to botnet C&C servers over a 1 month period

UNCOVERING BEHAVIOR

Looking at a list of IP's isn't immediately useful



```
250.248.131.219
249.64.58.255
252.48.31.24
255.80.130.120
248.144.82.156
46.165.220.155
69.64.147.10
46.165.229.165
114.215.98.58
171.122.62.97
169.58.184.33
250.96.181.92
171.250.1[illegible].3[illegible]
[illegible]
212.[illegible]27.20.93
170.18.108.134
216.239.32.21
173.236.55.90
[illegible]
46.165.220.152
46.165.254.193
46.165.254.197
89.223.109.60
89.223.109.60
89.223.109.60
46.165.254.194
46.165.254.193
81.169.145.162
52.0.217.44
185.66.236.14
217.70.142.74
203.151.233.116
202.254.234.141
255.32.117.121
46.165.220.145
46.165.220.145
176.53.118.145
37.9.175.13
```

CLEANING DATA

- Relationships between other indicators can develop intelligence on attack and botnet infrastructure

- Which behavior features would be interesting?
  - lat/lon
  - how many clients are visiting?
  - the first seen date of a particular ioc
  - connected infrastructure : ips, asns, domains, namerserver

CLEANING DATA

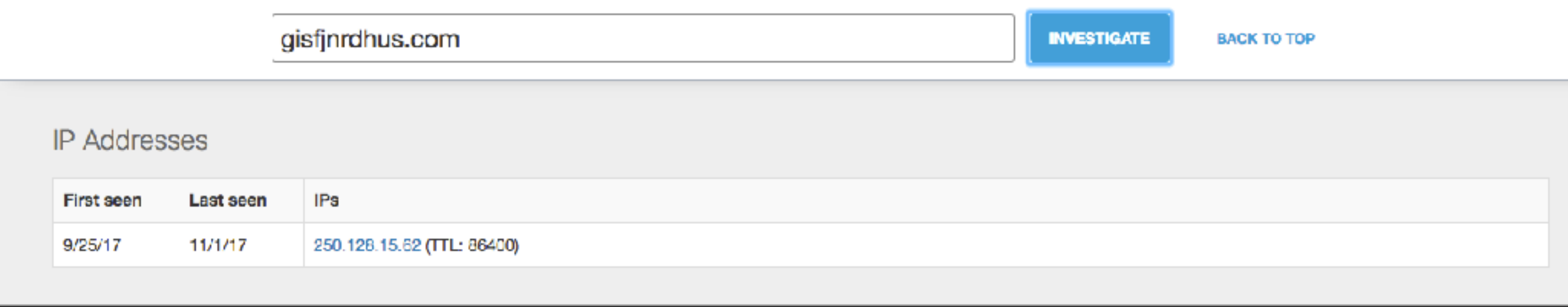
- Some are not connected and need cleaned out

127.0.0.1

8.8.8.8

255*

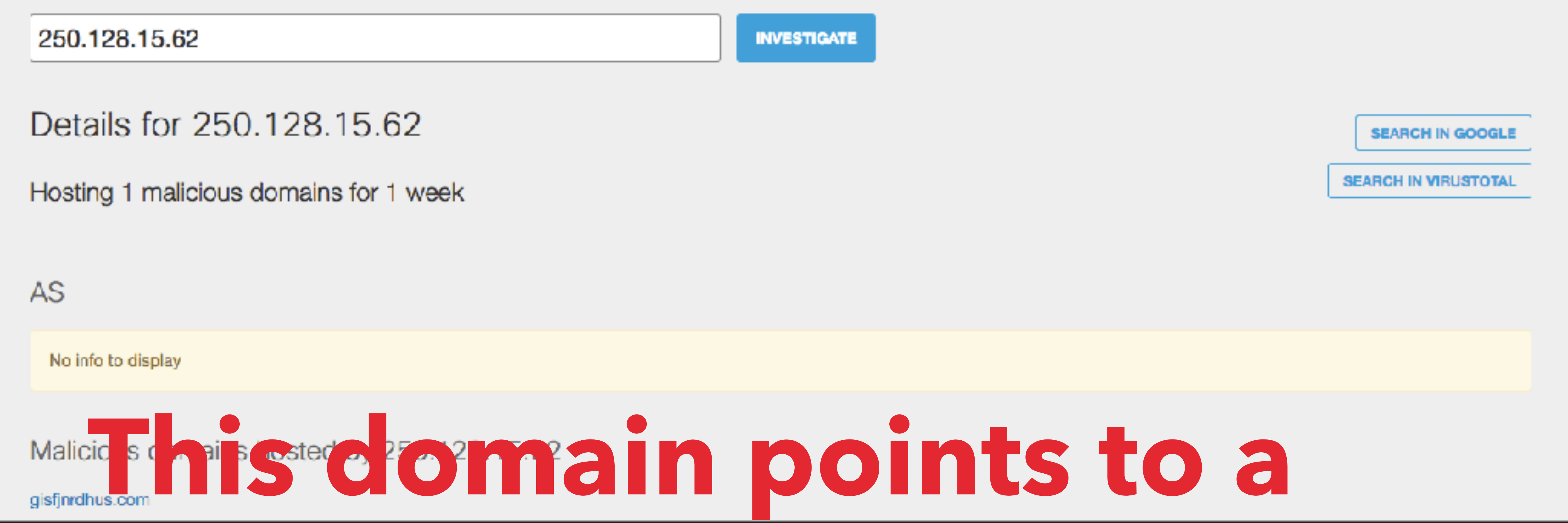
Get rid of data that doesn’t help



gisfjnrdhus.com

IP Addresses

First seen	Last seen	IPs
9/25/17	11/1/17	250.128.15.62 (TTL: 86400)



250.128.15.62

Details for 250.128.15.62

Hosting 1 malicious domains for 1 week

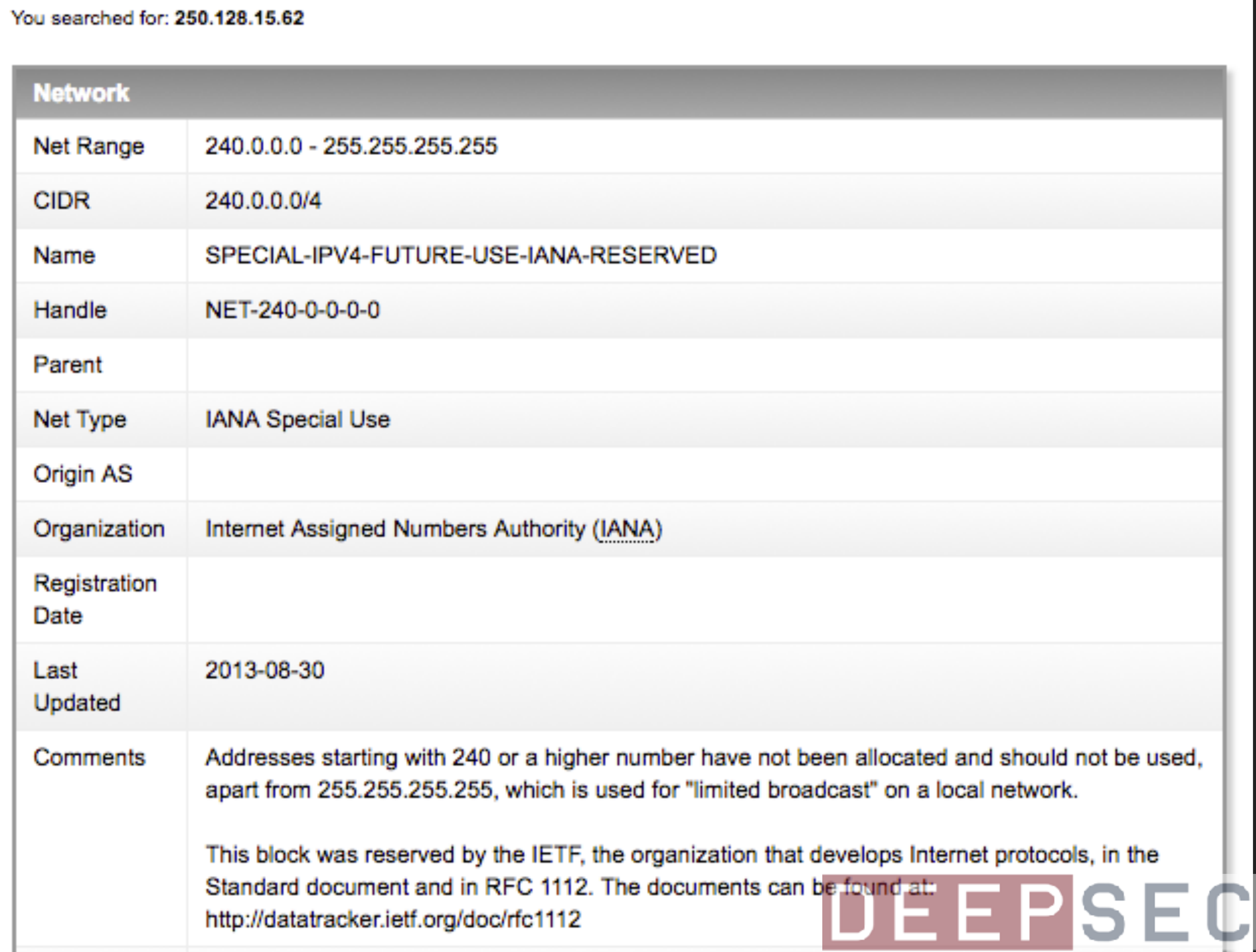
AS

No info to display

Malicious domains hosted by 250.128.15.62

gisfjnrdhus.com

This domain points to a reserved IP



You searched for: **250.128.15.62**

Network	
Net Range	240.0.0.0 - 255.255.255.255
CIDR	240.0.0.0/4
Name	SPECIAL-IPV4-FUTURE-USE-IANA-RESERVED
Handle	NET-240-0-0-0-0
Parent	
Net Type	IANA Special Use
Origin AS	
Organization	Internet Assigned Numbers Authority (IANA)
Registration Date	
Last Updated	2013-08-30
Comments	Addresses starting with 240 or a higher number have not been allocated and should not be used, apart from 255.255.255.255, which is used for "limited broadcast" on a local network. This block was reserved by the IETF, the organization that develops Internet protocols, in the Standard document and in RFC 1112. The documents can be found at: http://datatracker.ietf.org/doc/rfc1112

CLEANING DATA

- Some IPs are usually compromised webservers used to proxy/hide the C&C communications

Using Necurs as an example

NECURS BOTNET

NECURS BOTNET INSIDE STORY

- Infection Method
  - Spam with malicious attachments
  - Malvertising
  - Exploit Kits
  - Malicious links in emails

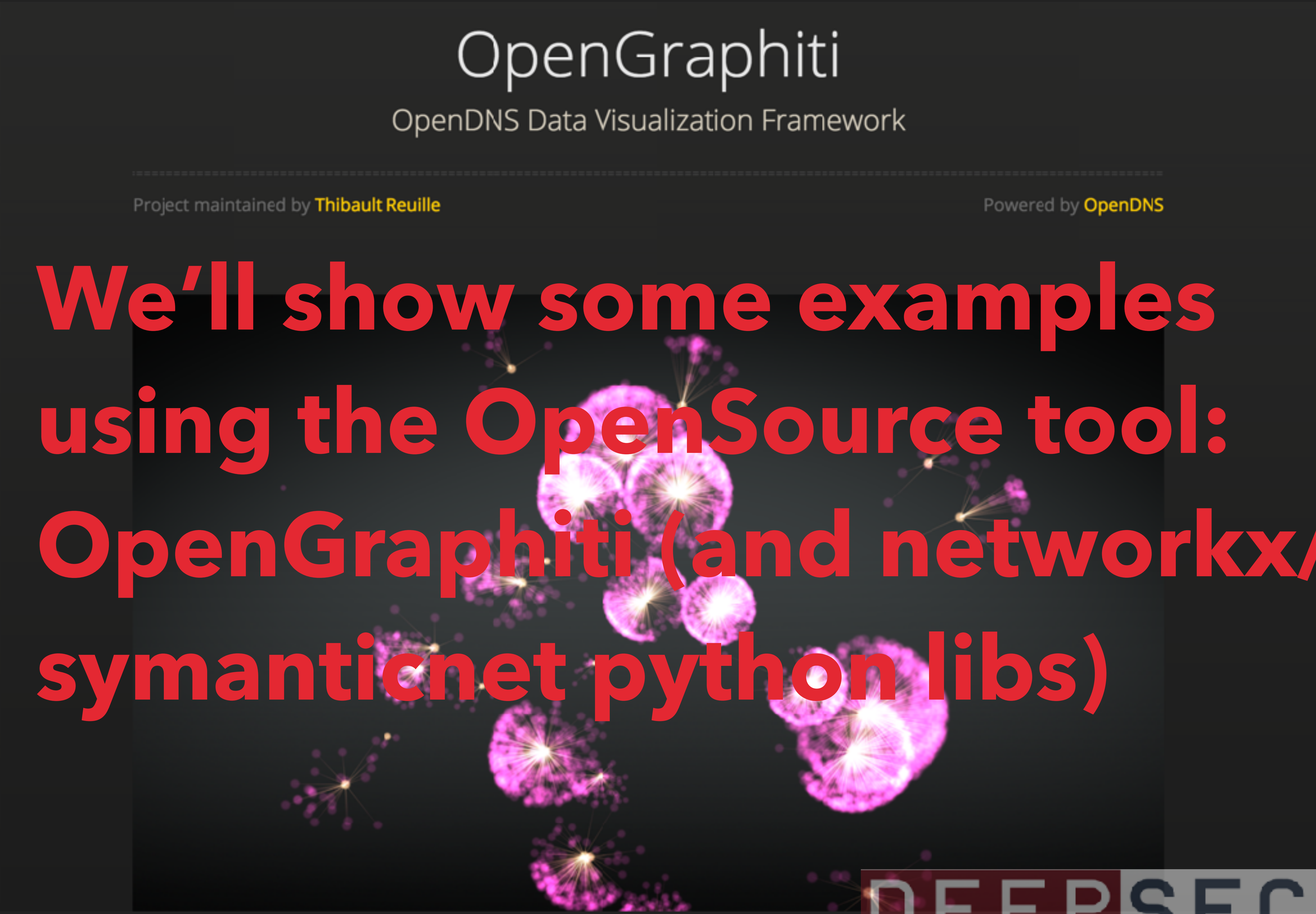
NECURS BOTNET INSIDE STORY

- <u>**Prominent Malware**</u>
  - **Ransomware**
  - **Banking Trojans**

NECURS BOTNET INSIDE STORY

- **Noteworthy**
  - DDoS ability
  - Uses 2 DGAs in effort to keep communications secret

CO-OCCURRING DGAS AND HOSTING IPS



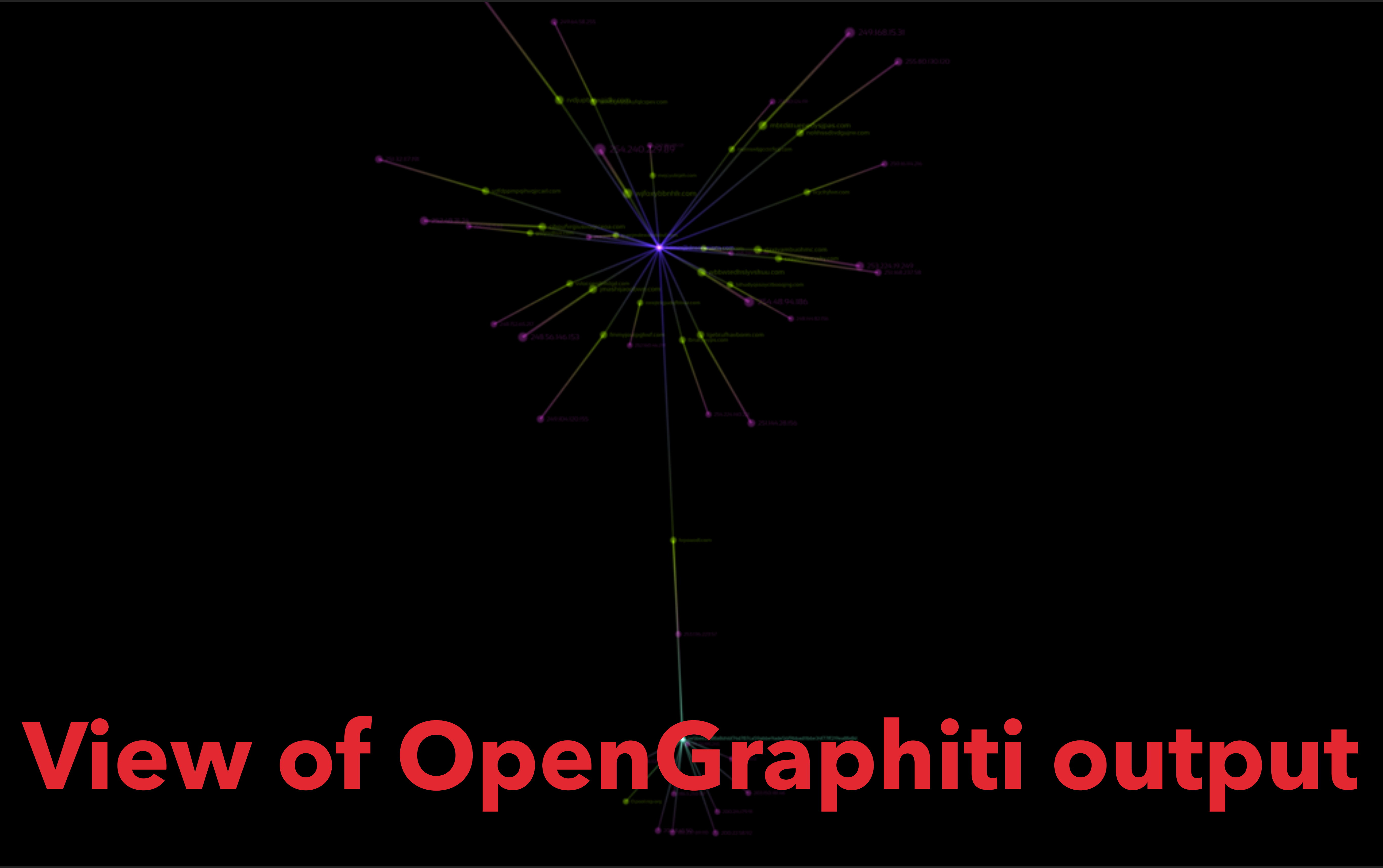
OpenGraphiti

OpenDNS Data Visualization Framework

Project maintained by Thibault Reuille

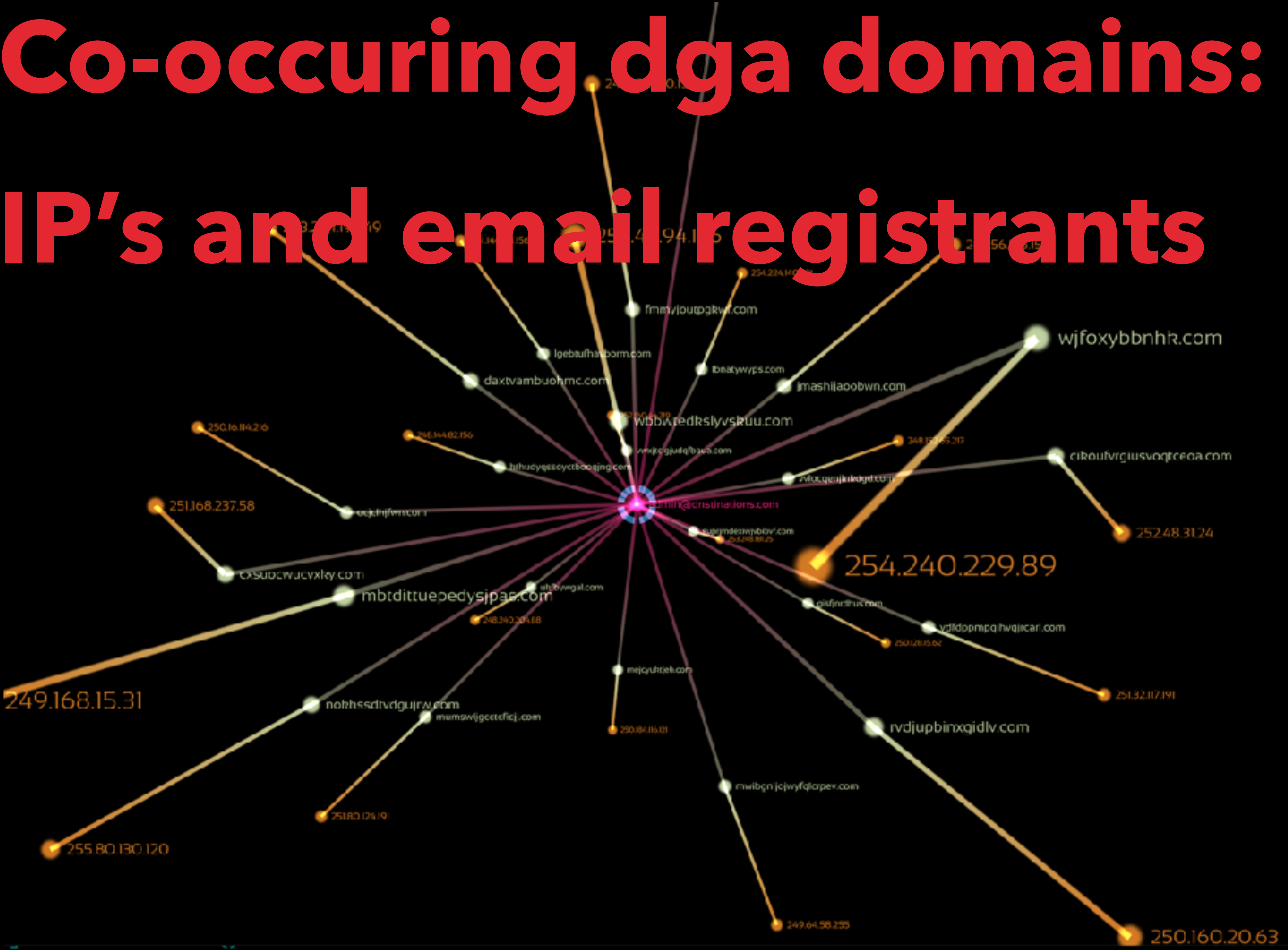
Powered by OpenDNS

We’ll show some examples using the OpenSource tool: OpenGraphiti (and networkx/ symanticnet python libs)

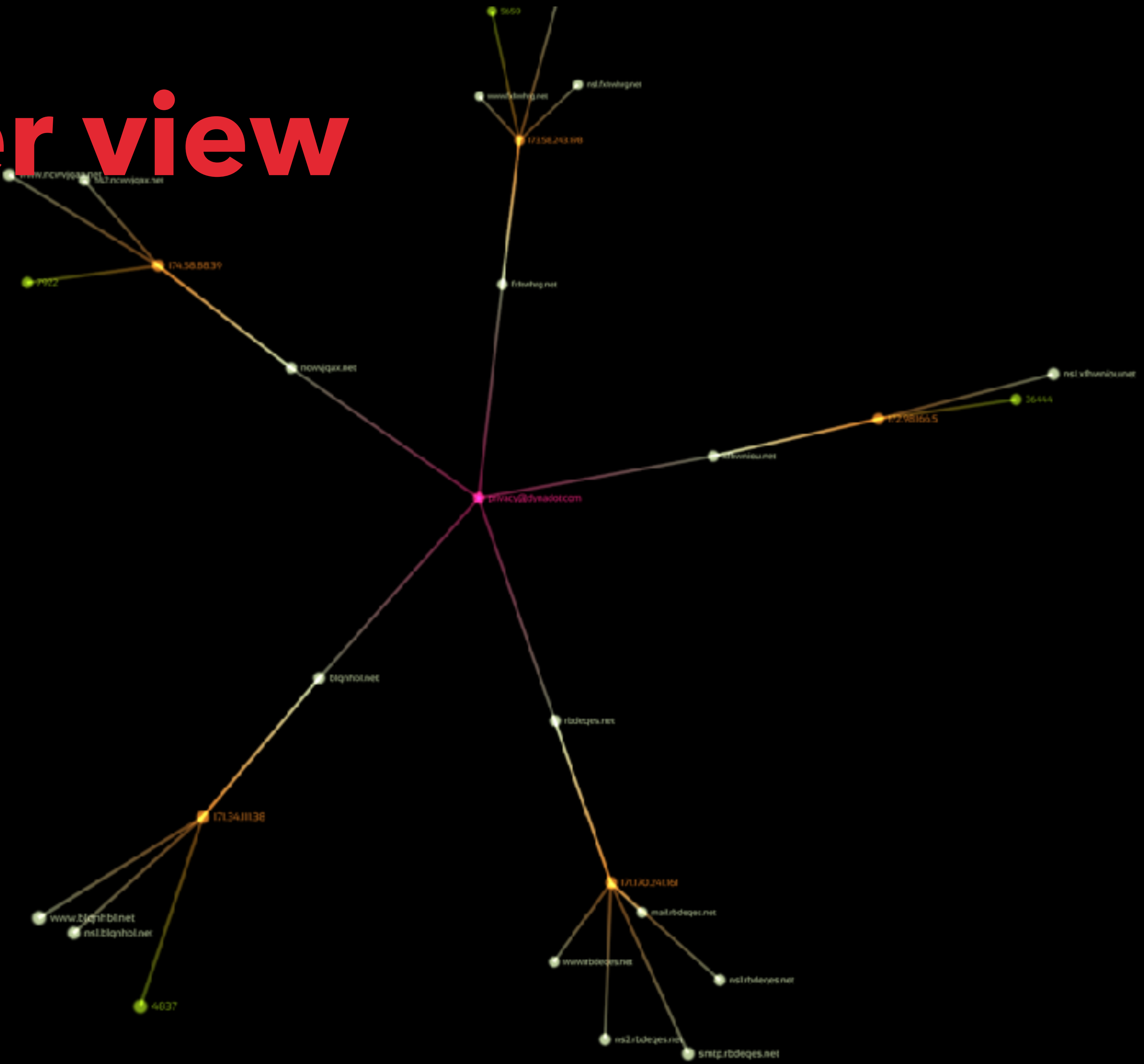


View of OpenGraphiti output

Co-occuring dga domains: IP’s and email registrants

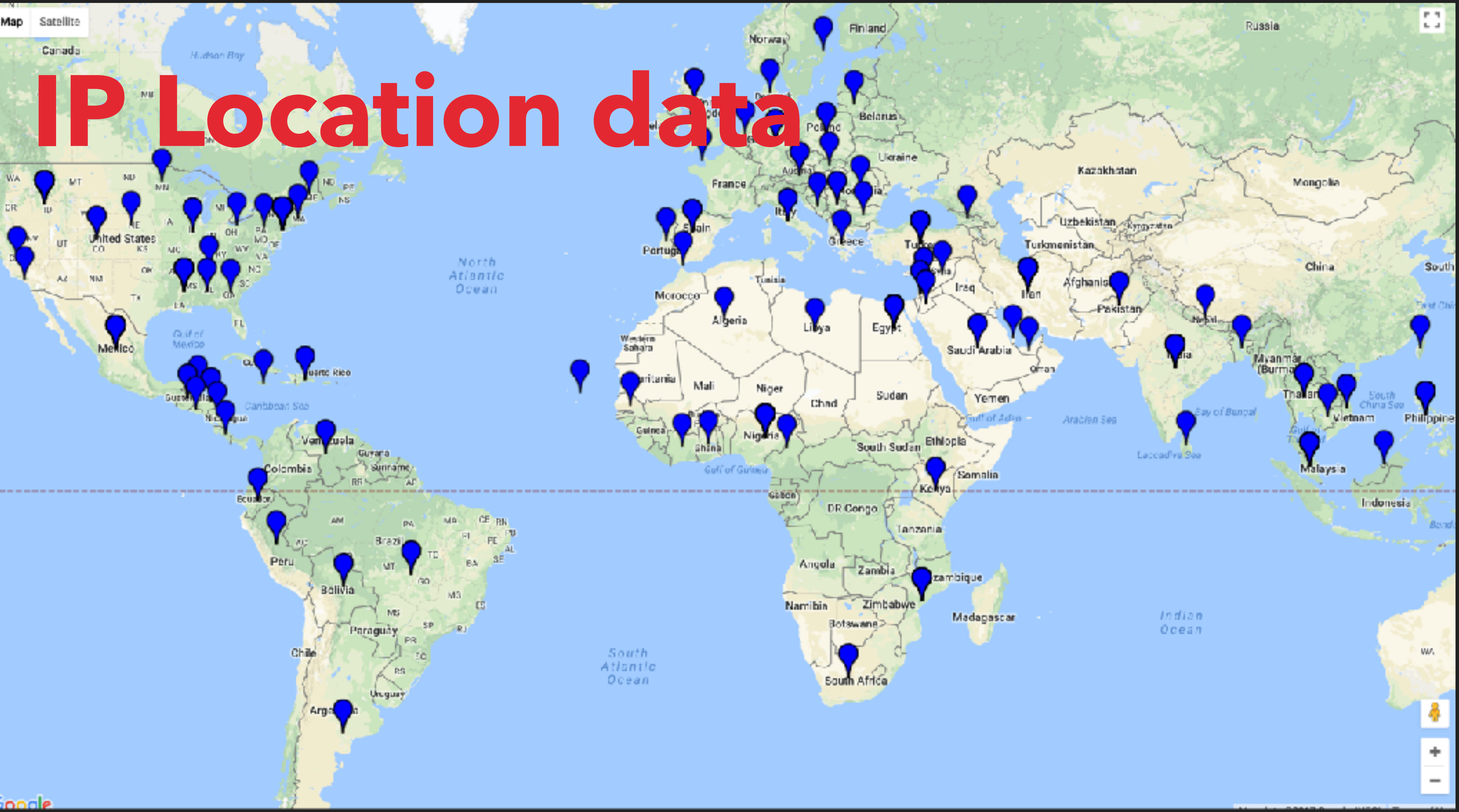


Another view



Co-occuring dga domains:

IP Location data



ATTACK CAMPAIGNS

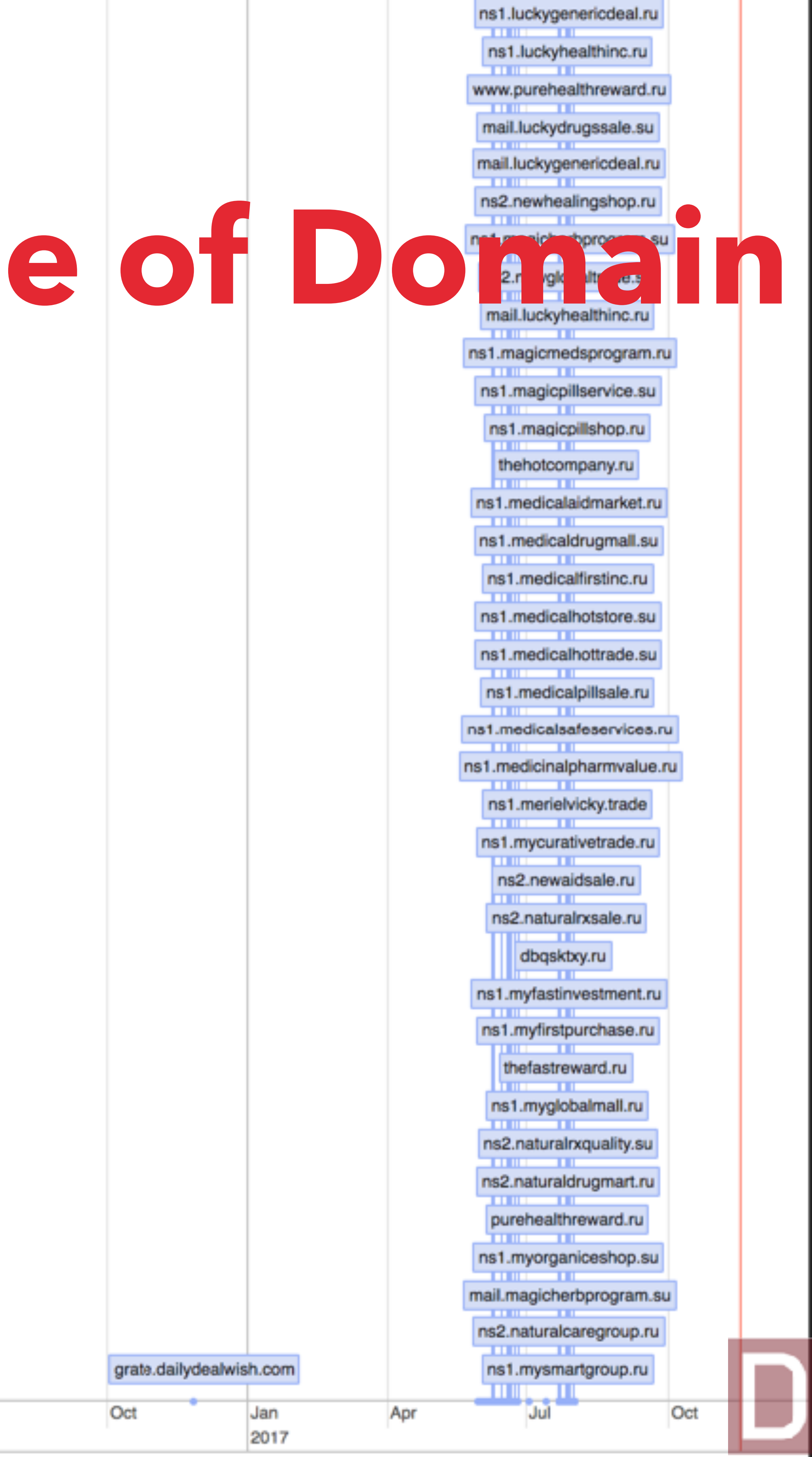
Using Globeimposter as an example

GLOBEIMPOSTER

HAILSTORM SPAM BOT SENDS GLOBEIMPOSTER

- **dategs[.]ru/js/tasok11[.]exe - from a hailstorm spam bot - 182.56.129.116 - Passive DNS**

Timeline of Domain use



HAILSTORM SPAM BOT SENDS GLOBEIMPOSTER

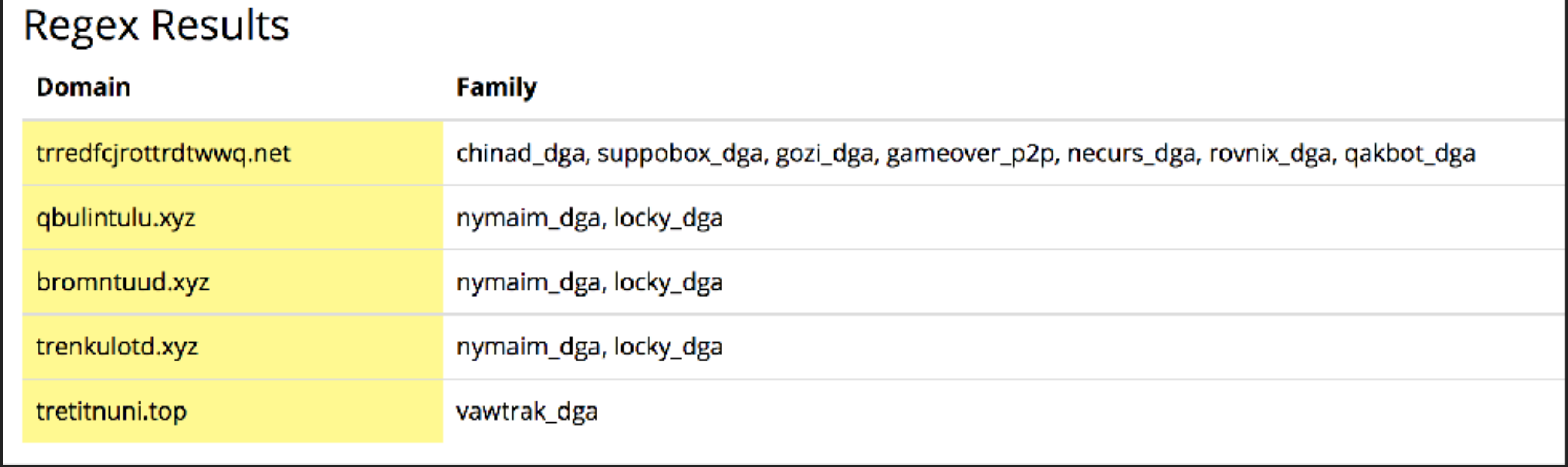
- 420855ef0326743f46da71127620be22089152c9029ba450d4f4679b8a8a122d - globeimposter

HAILSTORM SPAM BOT SENDS GLOBEIMPOSTER

- qbulintulu.xyz
- trenkulotd.xyz
- tretitnuni.top
- bromntuud.xyz

INFECTION AND SPREADING

- **DGArchive data - family regex matches**



Regex Results

Domain	Family
trredfcjrottrdtwwq.net	chinad_dga, suppobox_dga, gozi_dga, gameover_p2p, necurs_dga, rovnix_dga, qakbot_dga
qbulintulu.xyz	nymaim_dga, locky_dga
bromntuud.xyz	nymaim_dga, locky_dga
trenkulotd.xyz	nymaim_dga, locky_dga
tretitnuni.top	vawtrak_dga

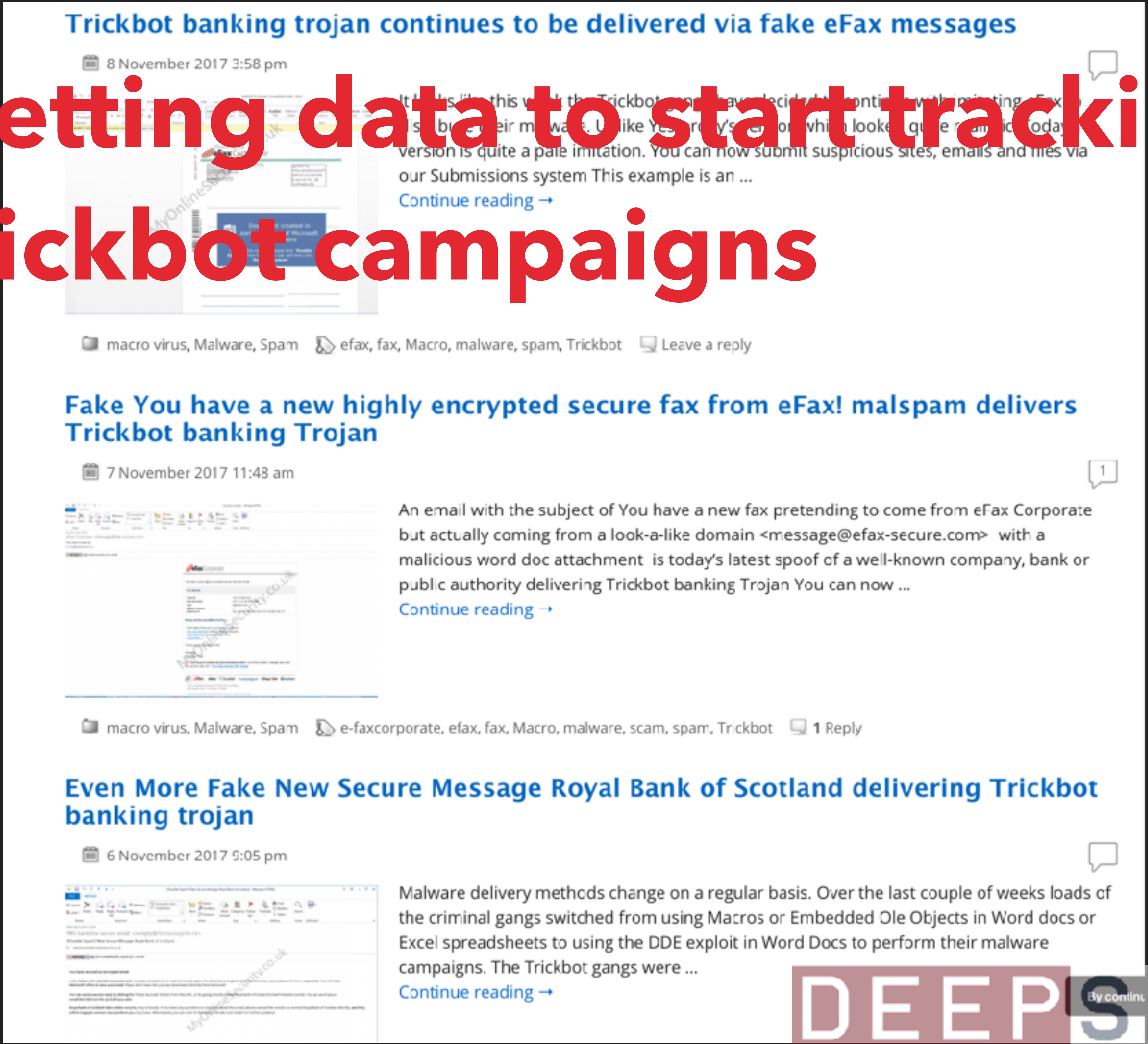
Using Trickbot as an example

TRICKBOT

C&C IP ADDRESSES AND RELATED HASHES

- Post infection trickbot tcp callouts - C&C
- How many hashes are related?
- myonlinesecurity.co.uk blogs about latest malspam pushes of trickbot

Getting data to start tracking trickbot campaigns



Trickbot banking trojan continues to be delivered via fake eFax messages

8 November 2017 3:58 pm

It looks like this week the Trickbot gang have decided to continue with imitating eFax to distribute their malware. Unlike Yesterday's version which looked quite realistic Today's version is quite a pale imitation. You can now submit suspicious sites, emails and files via our Submissions system This example is an …

Continue reading →

macro virus, Malware, Spam efax, fax, Macro, malware, spam, Trickbot Leave a reply

Fake You have a new highly encrypted secure fax from eFax! malspam delivers Trickbot banking Trojan

7 November 2017 11:48 am 1

An email with the subject of You have a new fax pretending to come from eFax Corporate but actually coming from a look-a-like domain <message@efax-secure.com> with a malicious word doc attachment is today's latest spoof of a well-known company, bank or public authority delivering Trickbot banking Trojan You can now …

Continue reading →

macro virus, Malware, Spam e-faxcorporate, efax, fax, Macro, malware, scam, spam, Trickbot 1 Reply

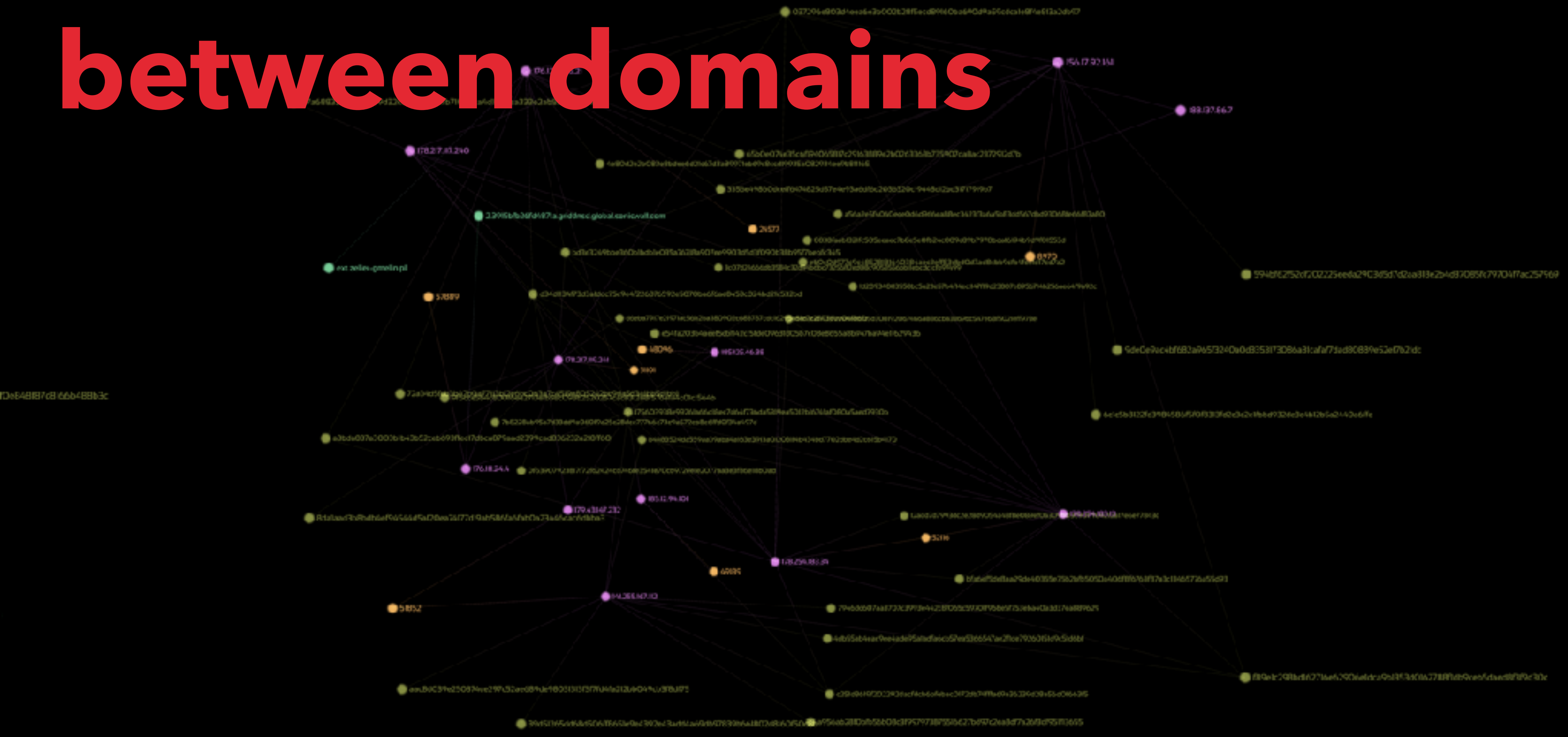
Even More Fake New Secure Message Royal Bank of Scotland delivering Trickbot banking trojan

6 November 2017 5:05 pm

Malware delivery methods change on a regular basis. Over the last couple of weeks loads of the criminal gangs switched from using Macros or Embedded Ole Objects in Word docs or Excel spreadsheets to using the DDE exploit in Word Docs to perform their malware campaigns. The Trickbot gangs were …

Continue reading →

Viewing connections between domains



Using Locky as an example

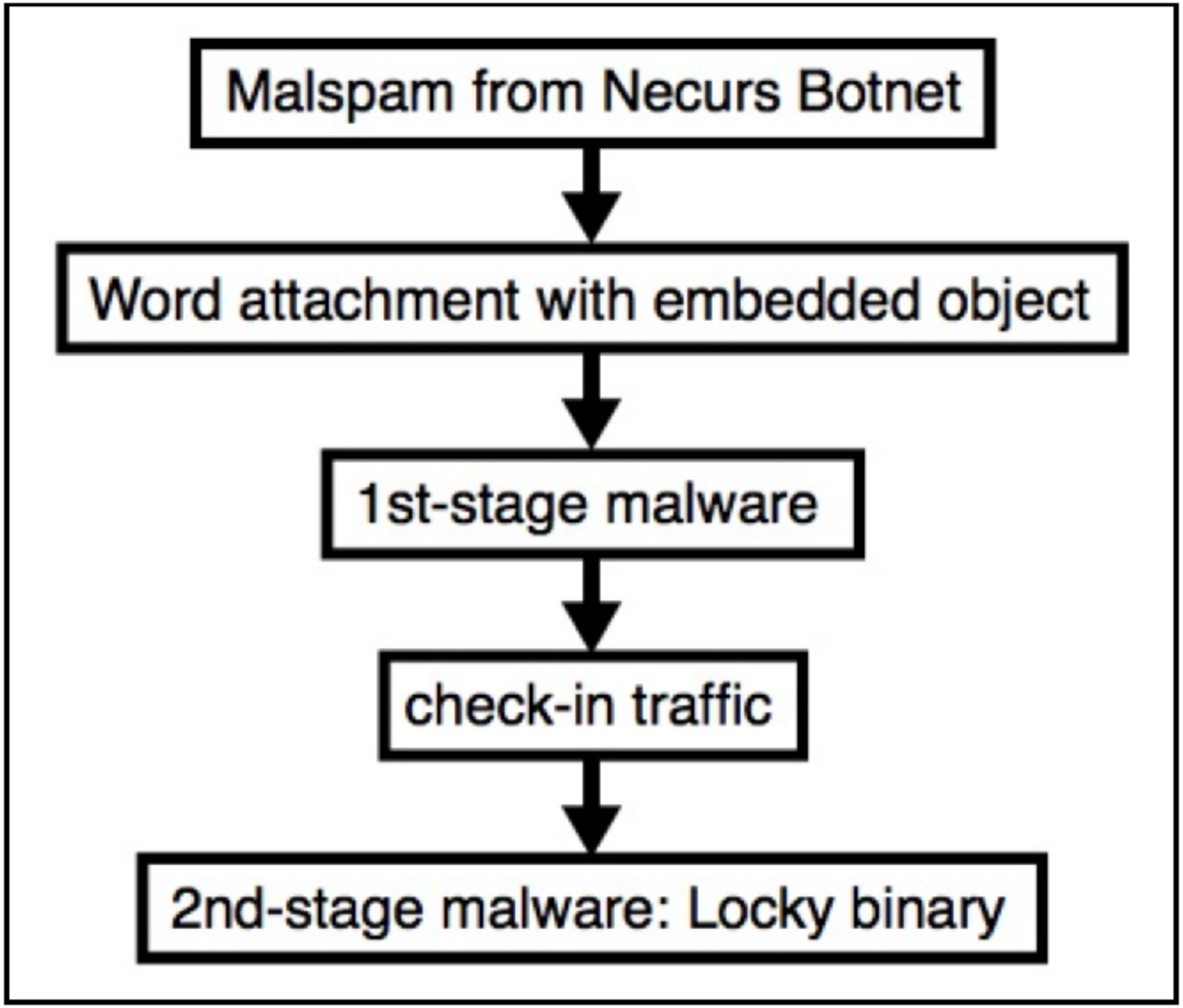
LOCKY

ONE HASH ALL THE THINGS

- necurs dgas + locky dgas (co-occurring) connects necurs with locky
- be5bee2088a8d46f74d787ca59abbe9ade56f9bbad11b6e34f77ff219ea8fe8d

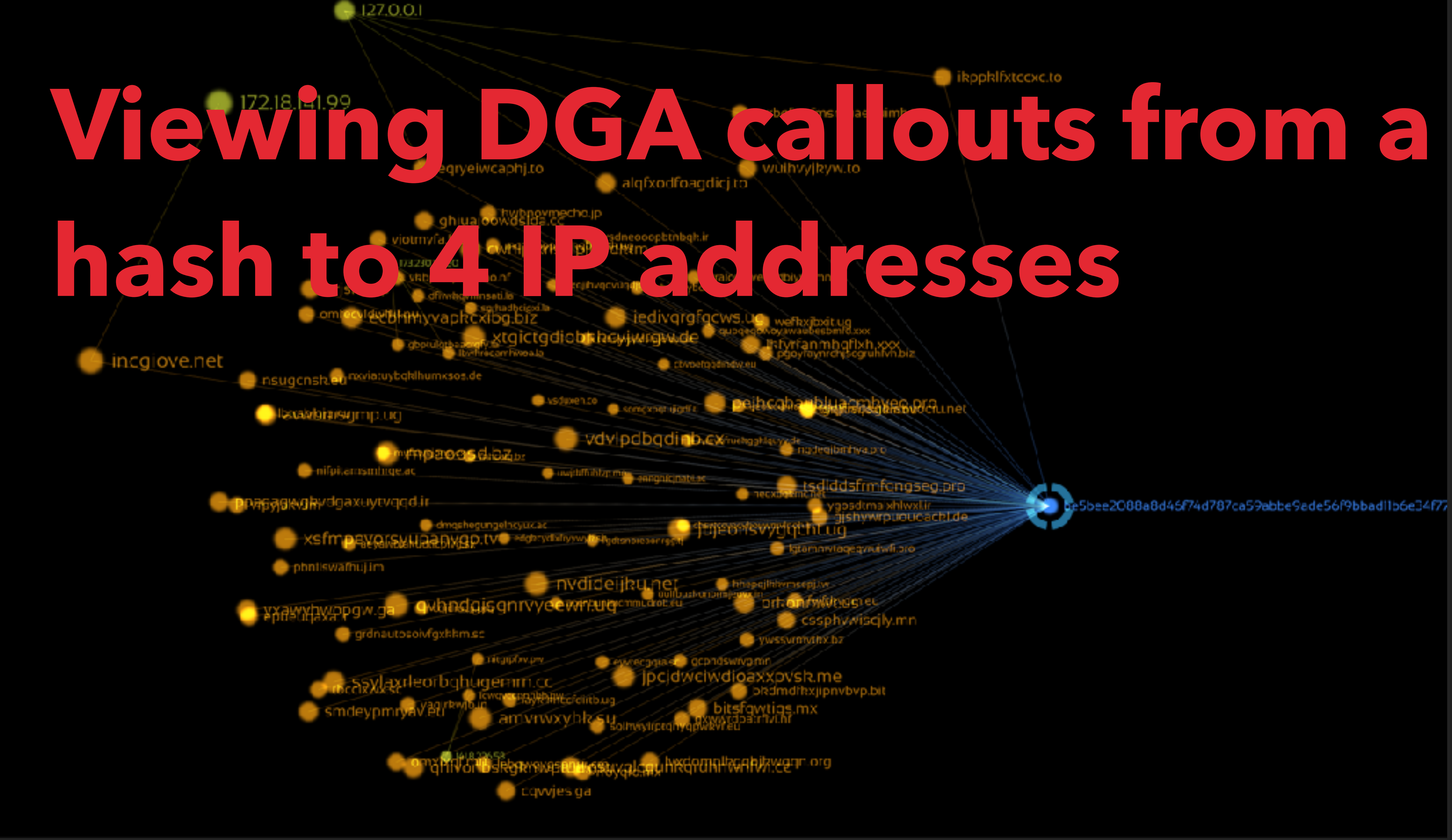
NOTES:

- Necurs Botnet malspam using embedded objects (not DDE attack) for the 2nd day in a row.
- Like yesterday, the Word documents have embedded objects that call Powershell to retreive the 1st-stage malware.

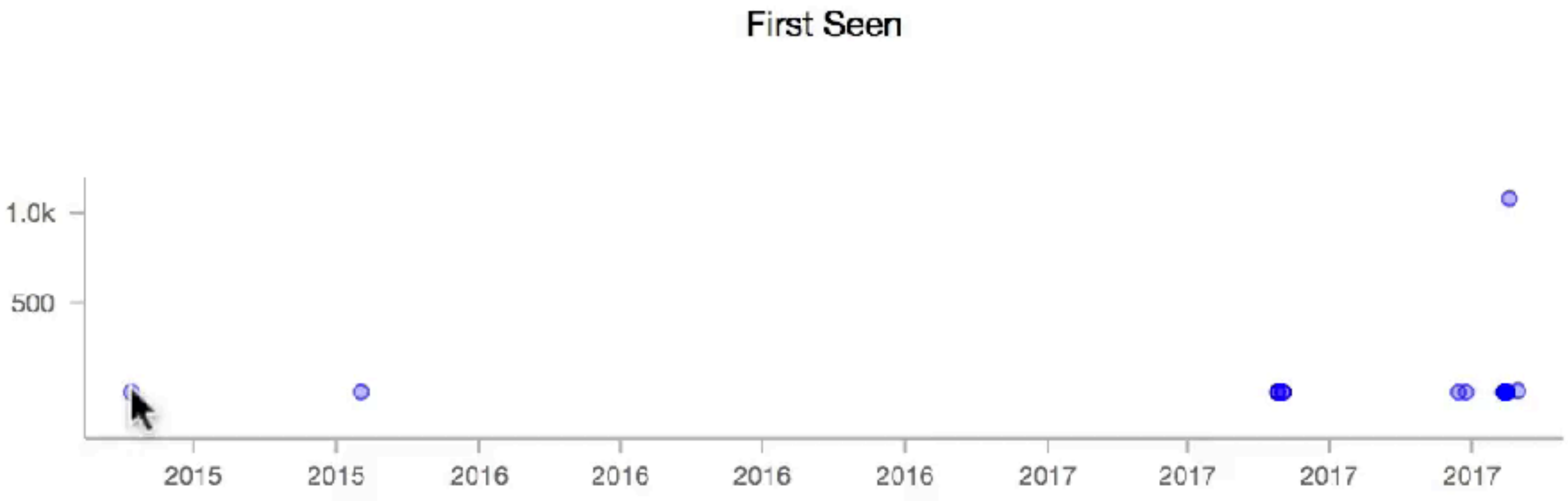

Malspam from Necurs Botnet
Word attachment with embedded object
1st-stage malware
check-in traffic
2nd-stage malware: Locky binary

Shown above: Current chain of events (no DDE, but embedded objects).

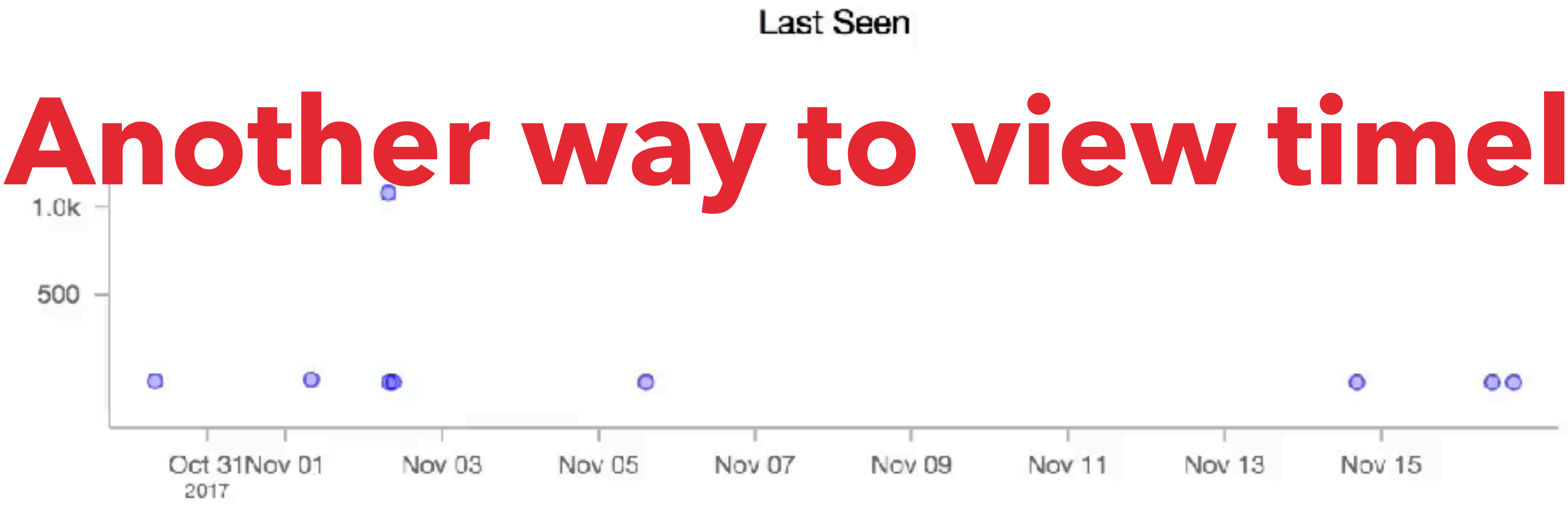
Viewing DGA callouts from a hash to 4 IP addresses



Another way to view timeline

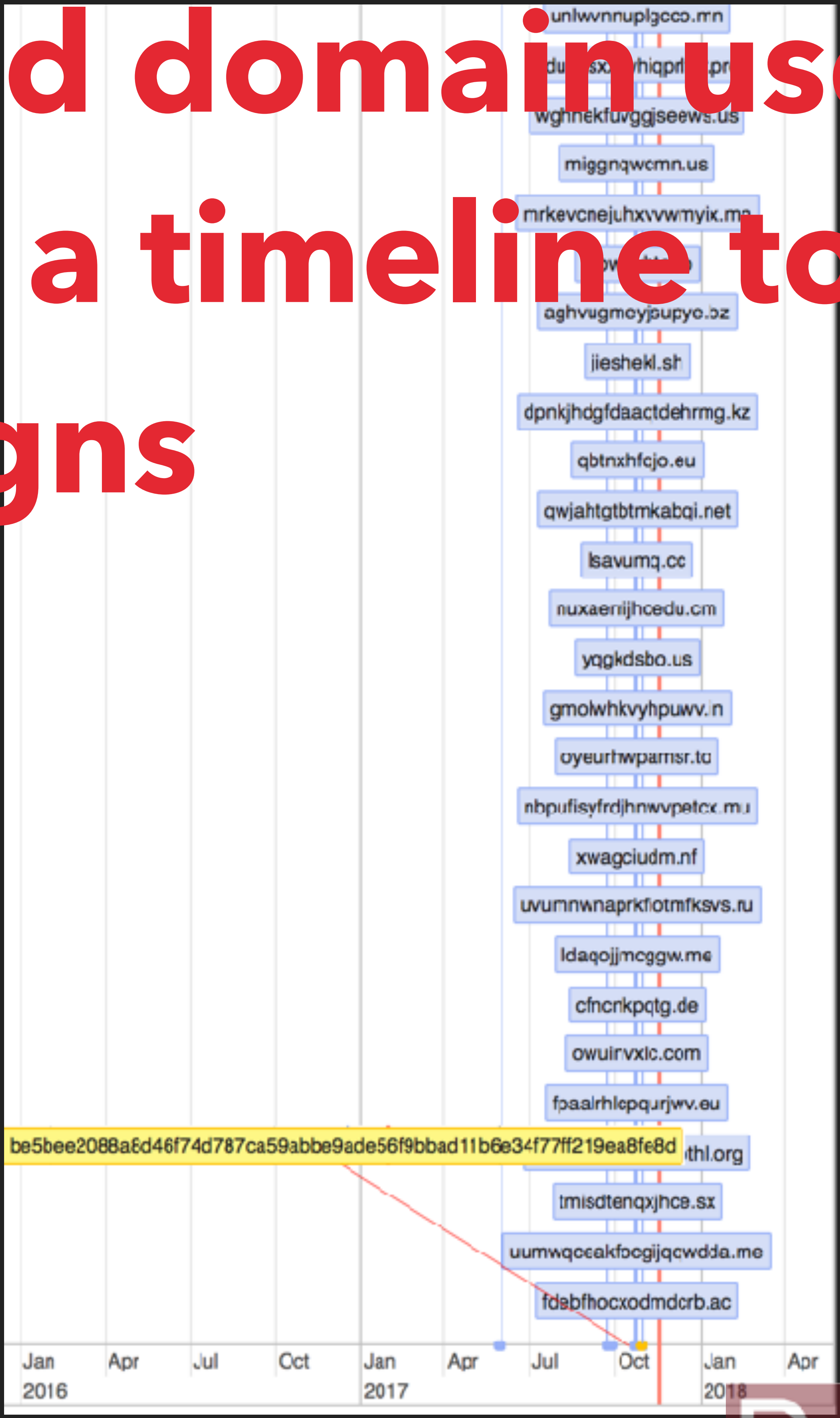


First Seen



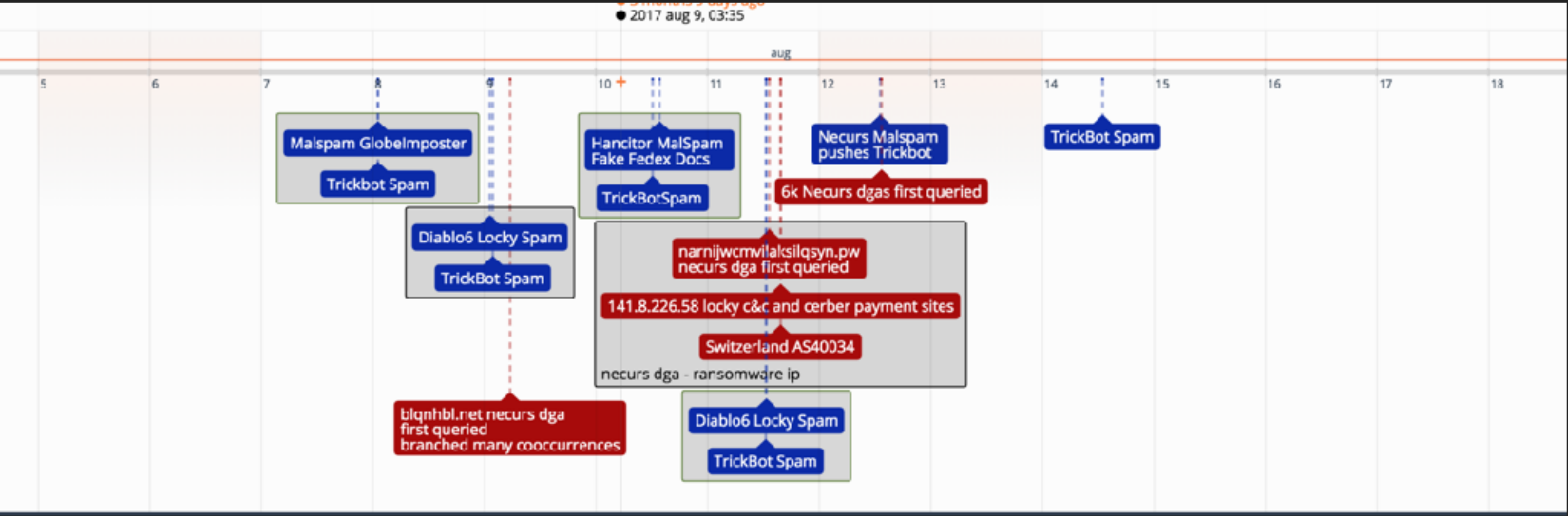
Last Seen

Hash and domain use by that hash on a timeline to track campaigns



ATTACK TIMELINE

Overall timeline of the attacks demonstrated in this presentation



Over long times, can be correlated with world events