UNCOVERING AND VISUALIZING MALICIOUS INFRASTRUCTURE

ABOUT US

ANDREA SCARFO

Security Research Manager & Security Researcher

Cisco Umbrella (formerly OpenDNS) in San Francisco.
Joined in 2015

OpenDNS

Cisco Umbrella

Previously:
System Administrator for 12 years

JOSH PYORRE

Senior Security Research Analyst & Security Researcher

Cisco Umbrella (formerly OpenDNS) in San Francisco.

Joined in 2015

OpenDNS

Cisco Umbrella

Previously:

NASA

MANDIANT

Consulting for Non-Profits:

Point Blue Conservation Science

Hamilton Families
HOUSING FIRST. COMMUNITY STRONG.

SUMMARY

- Our Research
- Finding Maliciousness
- Why Build Visualizations
- Visualizations and Findings

OUR RESEARCH

CRIMINAL ACTIVITY

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

SPAM

Mrs. Collete Gullo <qpemyyqlu@forthnet.gr> Sep 30

to me

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 my baby

[redacted]

h00kup now so send me msg
my screen name - **Collete87** ..
My account is here: http://czhonh.dategs.ru
Click and see my xxx album-
Collete87
I have much more sexy pics in the album above for you, my sweet :-* Call me!

WEBSITE COMPROMISE

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

RATS

Remote Access Trojans

WHAT IS THERE TO VISUALIZE?

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

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 good
goodpillscompany.su greg.jennylindi.eu gwennethjessika.ru homehealthvalue.su homeprivategroup.ru homeremedialinc.
hotglobalquality.su hprmfkay.curingbestmart.ru iantolna.homerxwebmart.ru ifafhtxg.thesmartwebmart.ru igdoonf.globalrx
janalainey.ru jarjkvua.newremedyelement.ru jcucwivh.newremedyelement.ru jjudokng.curingbestmart.ru jqqzpyuh.newren
kbofnhne.hotgenericsmart.ru kxwukygf.firstdrugmall.ru kzmnuxux.fastsmartbargain.ru lobdungy.medicalmedsgroup.ru lo
mail.bambyteriann.trade mail.pureaidvalue.ru mail.smartsecureinc.ru mail.xn--b1aht2abi5ap.xn--p1ai mail.xn--b1akwmvz
mail.xn--g1aiih0c9b.xn--p1ai medicaldrugsmall.su medicalhealthinc.su mlwndvrj.firstdrugmall.ru msilkryd.newremedyele

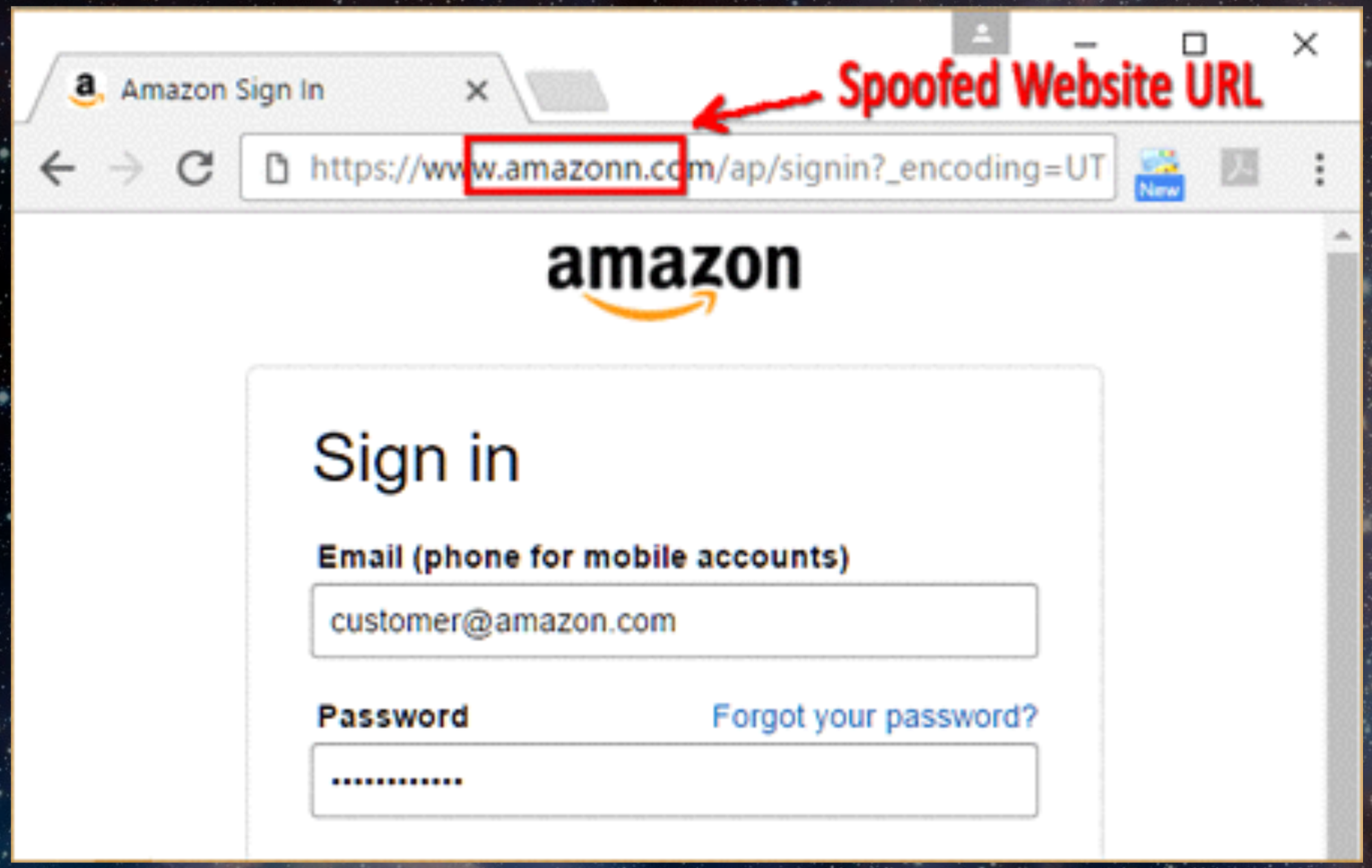
10.8.6.102	mihecksandca.ru	Client Hello
mihecksandca.ru	10.8.6.102	https → 49259 [ACK] Seq=1 Ack=190 Win=64240 Len=0
mihecksandca.ru	10.8.6.102	Server Hello, Certificate, Server Hello Done
10.8.6.102	mihecksandca.ru	49259 → https [ACK] Seq=190 Ack=970 Win=63271 Len=0
10.8.6.102	mihecksandca.ru	Client Key Exchange, Change Cipher Spec, Encrypted Handsha
mihecksandca.ru	10.8.6.102	https → 49259 [ACK] Seq=970 Ack=548 Win=64240 Len=0
mihecksandca.ru	10.8.6.102	Change Cipher Spec, Encrypted Handshake Message
10.8.6.102	mihecksandca.ru	49259 → https [ACK] Seq=548 Ack=1061 Win=63180 Len=0
10.8.6.102	mihecksandca.ru	Application Data
mihecksandca.ru	10.8.6.102	https → 49259 [ACK] Seq=1061 Ack=953 Win=64240 Len=0
10.8.6.102	mihecksandca.ru	Application Data
mihecksandca.ru	10.8.6.102	https → 49259 [ACK] Seq=1061 Ack=1742 Win=64240 Len=0
mihecksandca.ru	10.8.6.102	[TCP segment of a reassembled PDU]
mihecksandca.ru	10.8.6.102	[TCP segment of a reassembled PDU]

DEPENDS ON THE TYPE OF ATTACK

COMPROMISED DOMAINS

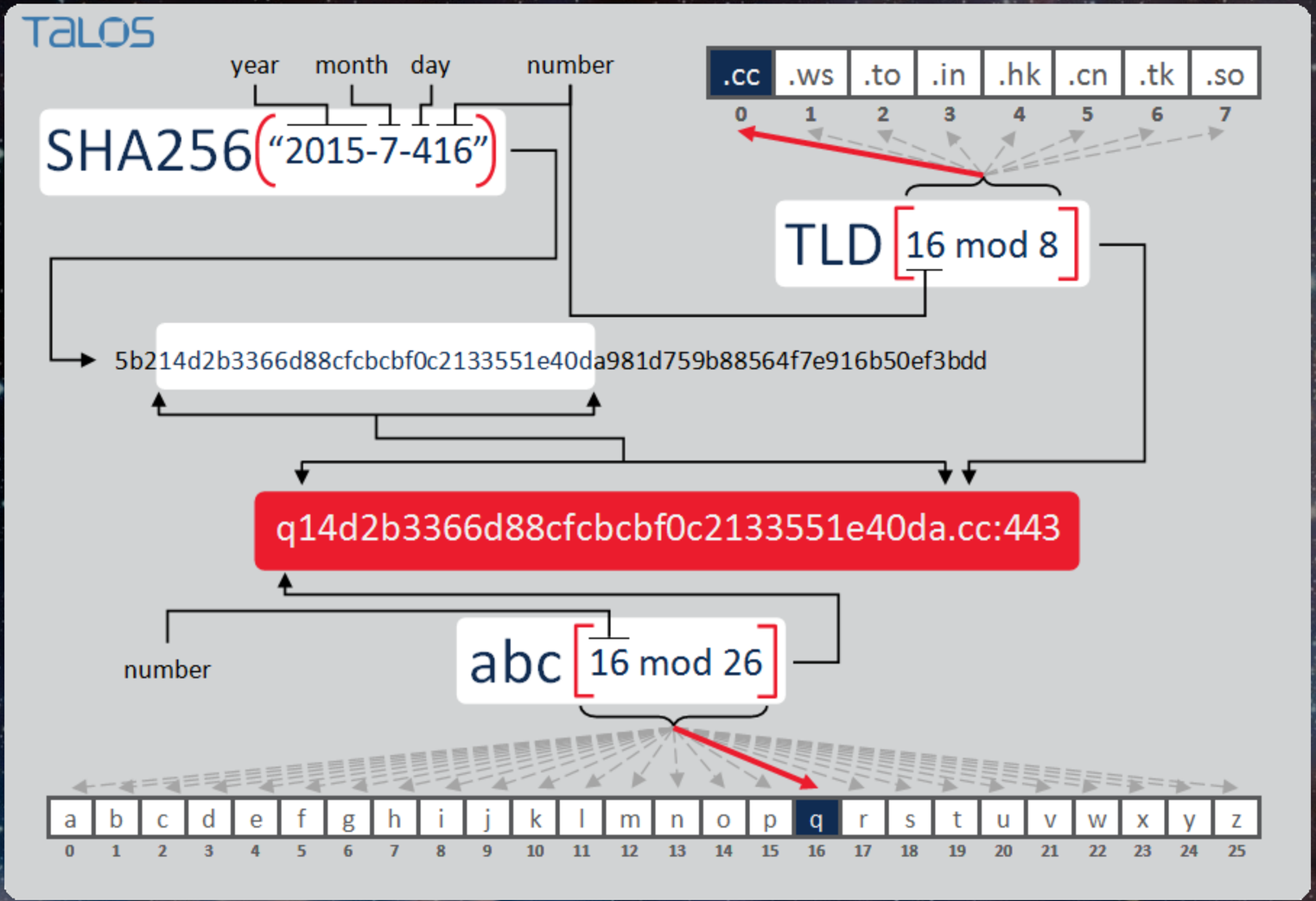
DEPENDS ON THE TYPE OF ATTACK

PHISHING DOMAINS



DEPENDS ON THE TYPE OF ATTACK

COMMAND & CONTROL DOMAINS (DGAS)

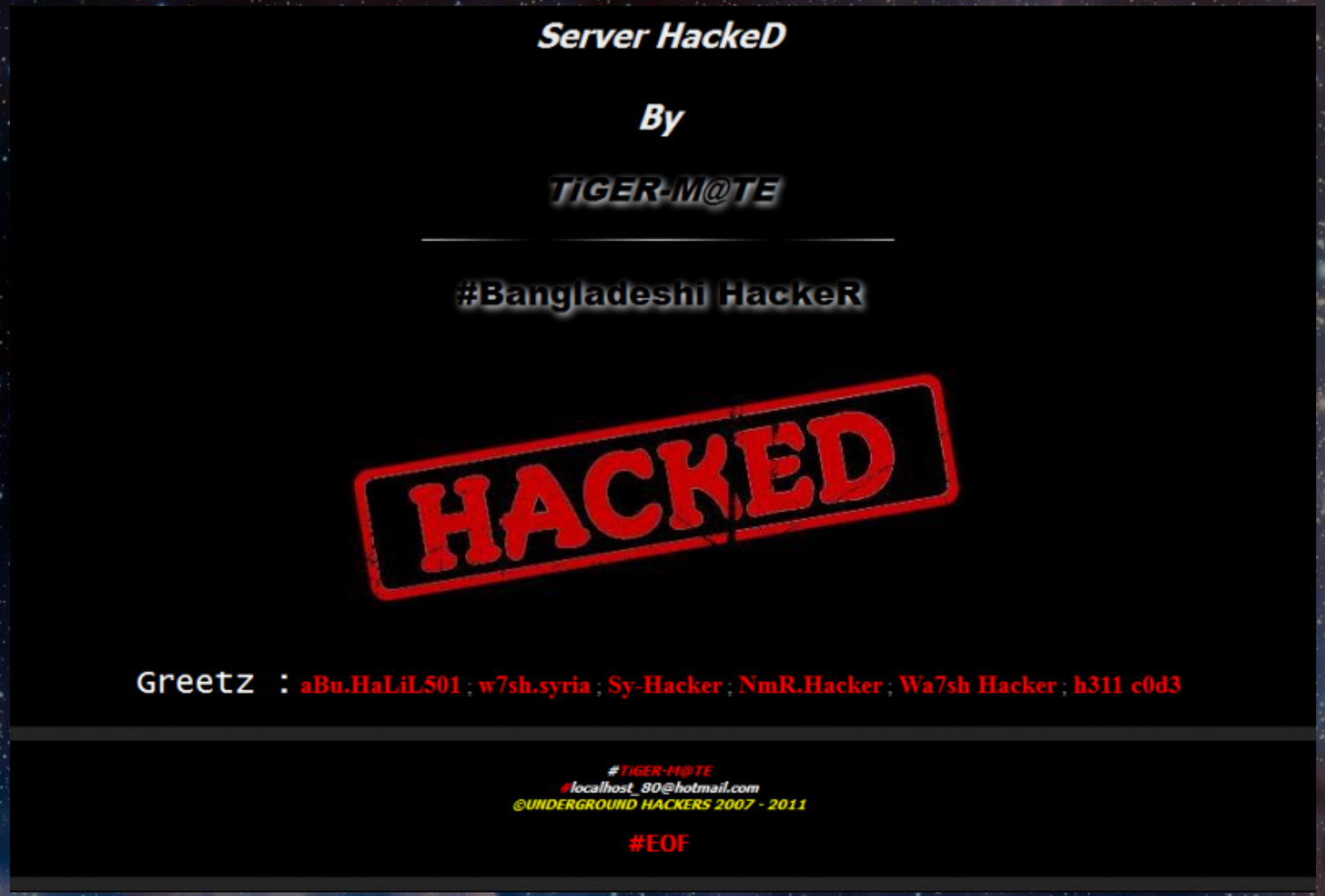


DEPENDS ON THE INFECTION METHOD

SPAM

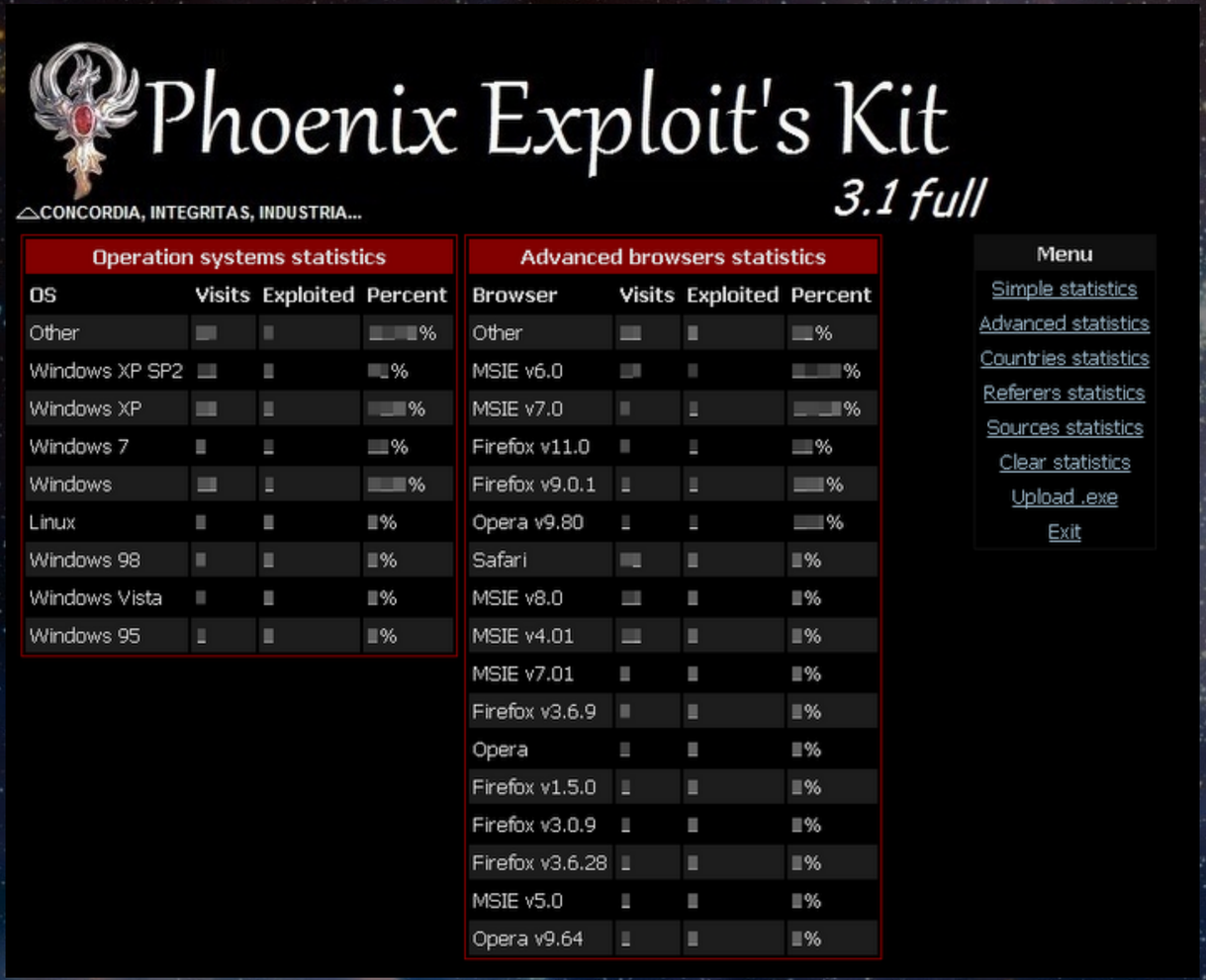
DEPENDS ON THE INFECTION METHOD

WEBSITE COMPROMISE



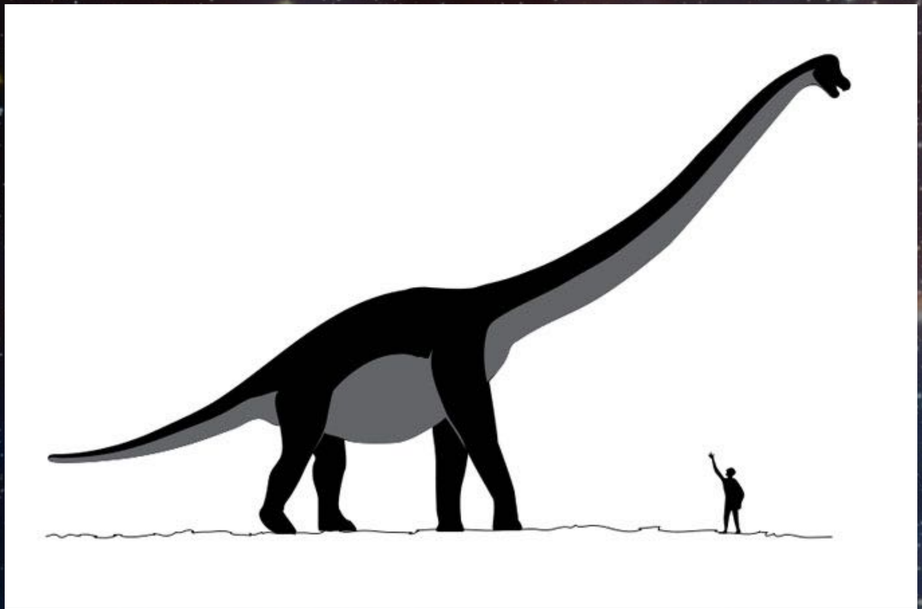
DEPENDS ON THE INFECTION METHOD

EXPLOIT KITS



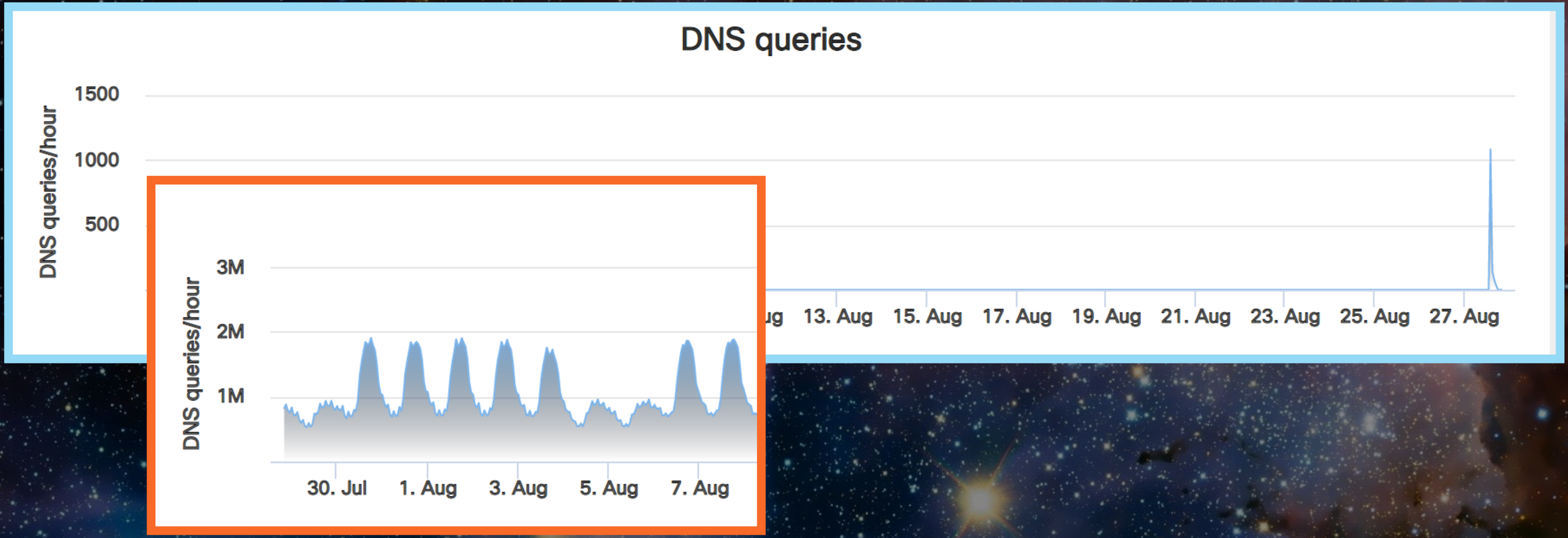
REACH

SIZE and SCALE



FEATURES FROM THE IOCS

2017-07-04 www.magicpharmacyinc.su



FINDING MALICIOUSNESS

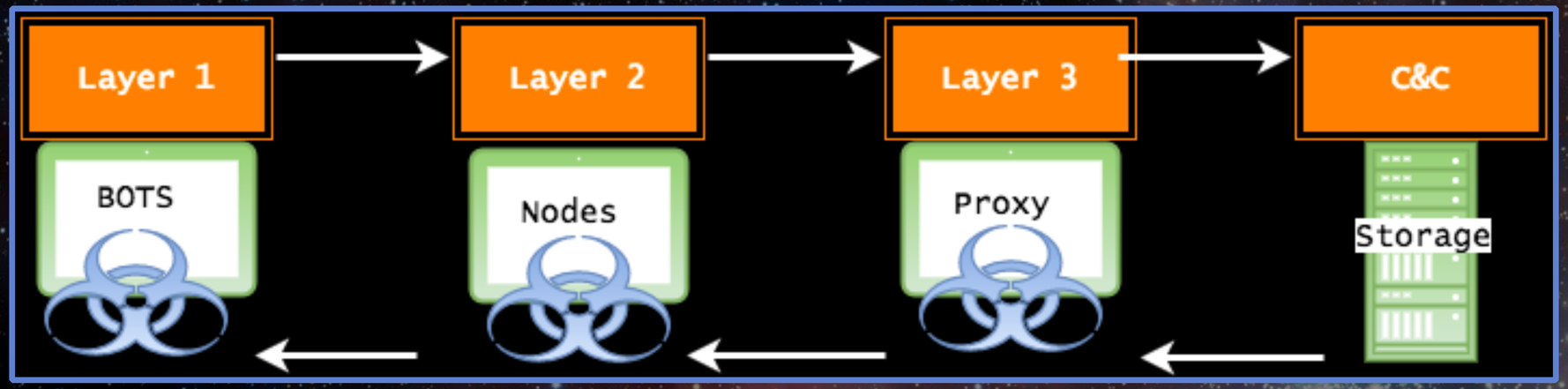
ANALYZING DGAS TO FIND THE C&C

Terminal Shell Edit View Window Help

ips_ccs_all_mongo_bo

```
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.net
ejwmxjttljbe.com
kevincolemanaerosports.com
paraondeissovai.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
```

EXAMPLE OF C&C CONTACT



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

C&C CONTACT - DOMAIN FLUX

- Large amount of changing DGA domains
- NX Domains
- Not all are registered - lots of noise to dig through
- One of the DGAs will be the C&C with a hosted IP address

PASSIVE DNS

- 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

Tracking Hailstorm Spam

USING PASSIVE DNS

95.31.22.193

95.31.22.193

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

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 firstho
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 h **SELECT DOMAINS SHOW PHARMA-SPAM DOMAINS** ebmart.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
ns1.blondelleevvy.ru ns1.brendaalmira.trade ns1.curingbestmart.ru ns1.curingremedymart.ru ns1.decioldb.ru ns1.denapa
ns1.firstdrugmall.ru ns1.globalrxprogram.ru ns1.goodgenericmall.su ns1.homerxwebmart.ru ns1.homesecureassist.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

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

WE CAN PIVOT AND FIND EVEN MORE DATA

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	zonnyasheelagh.eu
2017-08-01	zptcuhed.ru
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

WE CAN PIVOT AGAIN AND FIND EVEN MORE DATA

Details for lkvxmbtxsbiqp.com

SEARCH IN GOOGLE

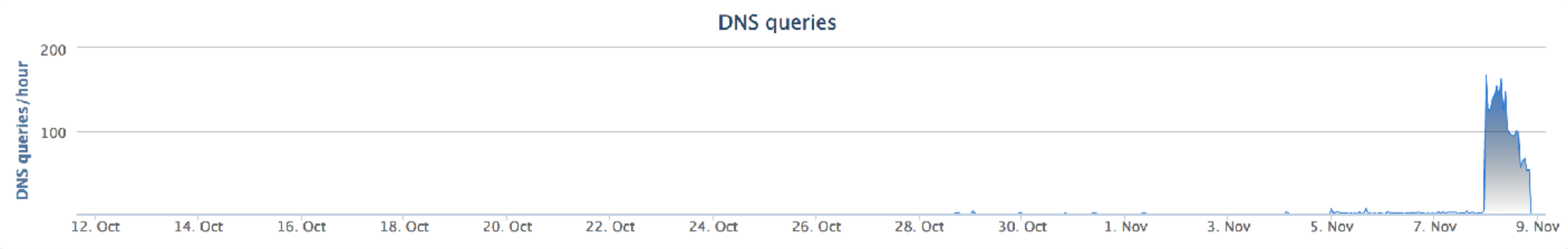
SEARCH IN VIRUSTOTAL

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)



WHOIS Record Data

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

Last retrieved October 28, 2017 GET LATEST

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

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

Details for lkvxmbtxsbiqp.com

SEARCH IN GOOGLE

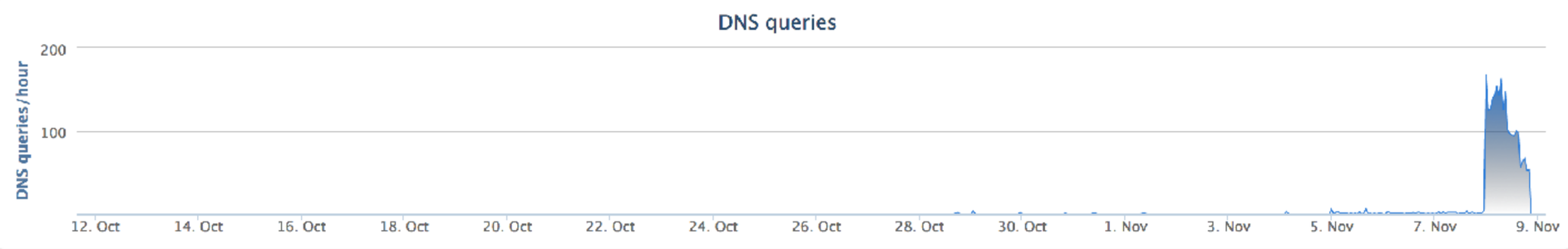
SEARCH IN VIRUSTOTAL

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)



IP Addresses

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

Details for lkvxmbtxsbiqp.com

SEARCH IN GOOGLE

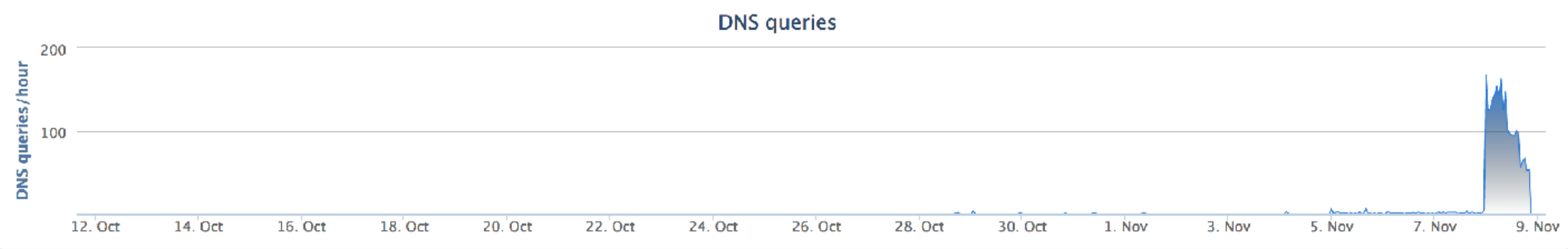
SEARCH IN VIRUSTOTAL

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)



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

Details for lkvxmbtxsbiqp.com

SEARCH IN GOOGLE

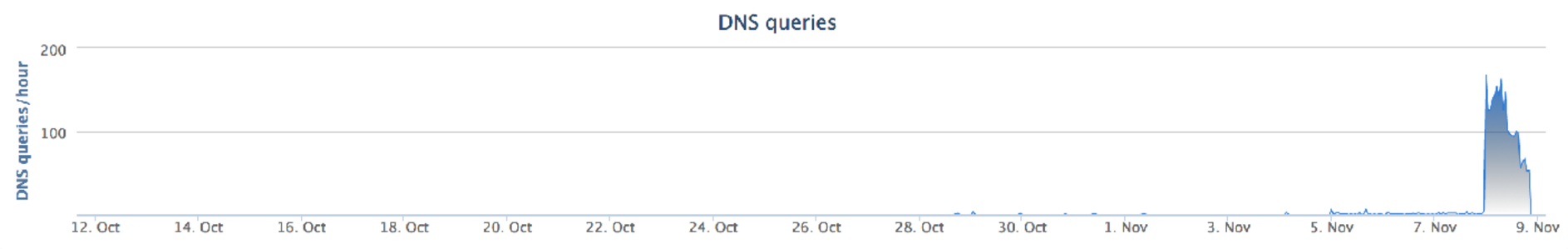
SEARCH IN VIRUSTOTAL

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 %)

CO-OCCURRING DOMAINS ARE QUERIED JUST BEFORE OR AFTER A DOMAIN

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)

OSINT

WHERE DO YOU GET DATA TO LOOK AT?

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 -- ElTest 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 ElTest 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

MALWARE-TRAFFIC-ANALYSIS.NET

2018-08-24 - QUICK POST: EMOTET INFECTIONS WITH ZEUS PANDA BANKER

ASSOCIATED FILES:

- **2018-08-22-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 2.1 MB (2,123,581 bytes)
- **2018-08-22-malware-from-Emotet-and-Zeus-Panda-Banker-infection.zip** 377 kB (377,181 bytes)

- **2018-08-24-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 1.3 MB (1,250,753 bytes)
- **2018-08-24-malware-from-Emotet-and-Zeus-Panda-Banker-infection.zip** 350 kB (349,531 bytes)

NOTES:

- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

http.request or ssl.handshake.type ==1 Expression... +

Time	Dst	port	Host	Server Name	Info
2018-08-22 14:49…	69.162.107.34	80	kofye.com		GET /FILE/En/Paid-Invoic
2018-08-22 14:49…	69.162.107.34	80	kofye.com		GET /FILE/En/Paid-Invoic
2018-08-22 14:49…	103.208.27.150	80	jobarba.com		GET /wp-content/dstf6 HT
2018-08-22 14:49…	103.208.27.150	80	jobarba.com		GET /wp-content/dstf6/ H
2018-08-22 14:50…	2.50.151.42	443	2.50.151.42:443		GET / HTTP/1.1
2018-08-22 14:52…	96.70.33.201	80	96.70.33.201		GET / HTTP/1.1
2018-08-22 14:53…	199.0.205.95	443	199.0.205.95:443		GET / HTTP/1.1
2018-08-22 14:57…	24.116.195.90	50…	24.116.195.90:50000		GET / HTTP/1.1
2018-08-22 14:58…	194.150.118.8	443	194.150.118.8:443		GET / HTTP/1.1
2018-08-22 14:58…	194.150.118.8	443	194.150.118.8:443		GET / HTTP/1.1
2018-08-22 14:58…	72.77.1.8	80…	72.77.1.8:8080		GET /whoami.php HTTP/1.1
2018-08-22 14:58…	72.77.1.8	80…	72.77.1.8:8080		POST / HTTP/1.1
2018-08-22 15:00…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:00…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:00…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:00…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:05…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:05…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:05…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:05…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:10…	172.217.9.164	443		www.google.com	Client Hello
2018-08-22 15:10…	178.132.7.106	443		sourieuse.website	Client Hello
2018-08-22 15:10…	178.132.7.106	443		sourieuse.website	Client Hello

DOMAINS FROM A PCAP

```
astraclinic.com
trustsoft.ro
tailbackuisback.xyz
mykeeptake.xyz
kermain-valley.com
tonysmarineservice.co.uk
canevazzi.com.br
fufu.com.mx
cranmorelodge.co.uk
weliketomoveit.ca
fundacionafanic.com
humoronoff.top
www.kirk666.top
nebula-ent.com
```

IT'S FASTER TO PROGRAMMATICALLY PULL DATA OUT OF A PCAP

```
gator3110.hostgator.com
www.thesocialindian.in
abovecreative.com
gmokkasd.website
alberguetaull.com
melissakiss.com
grupoembatec.com
amedion.net
vudoshakar123123.website
eeodlewnia.pl
simcon.ca
sano.ir
organicprom.ru
akademia.gnatyshyn.pl
soportek.cl
```

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

7 November 2017 8:21 pm

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 →

ANOTHER EXAMPLE OF A SITE WITH INTEL YOU COULD USE

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 →

DGARCHIVE

Fraunhofer FKIE

Instant Lookup | API Usage | Feedback | Malware Families | Changelog | Terms of Service

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					
3					
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

ANOTHER EXAMPLE OF A SITE WITH INTEL YOU COULD USE

VirusTotal

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

File | URL | Search

ANOTHER EXAMPLE OF A SITE WITH INTEL YOU COULD USE

Upload and scan file

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.

Secure https://www.virustotal.com/intelligence/search/?query=humoronoff.top

Search Hunting Clustering Statistics Help New joshpyorre

virustotal intelligence

humoronoff.top Search Hashes Select Download

4 files found

File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
a96ba206cbe2bc4b0835d2adf5355674e8681e19f4113da34f2c804d8bebc257	50 / 68	2018-08-01	2018-08-09	2	2	173.5 KB
cebf4fa9c2b7d855d4901174645a3286dbdf4f0f55c2082e184a9aa892ed707d aab3523f3b4c2b79668a2e33d3eb9d85 peexe overlay	49 / 69	2018-08-06 18:11:46	2018-08-06 18:11:46	1	1	173.5 KB
20f4445b40dc0cd1830dee6031a7342284e51dc4c399d331507b28f74ba0727b acfadcf7242b6d20d76d925b8c15faeb peexe	52 / 68	2018-07-31 14:57:13	2018-08-02 15:07:13	3	3	133.5 KB
64f7bb1f34a76c3f145f4e5f2b73bba217b781dafbf13709a228ba53c3c13f4f f7487033b109cf0b34e448d77a29e457 cap malware trojan	0 / 59	2018-08-02 15:06:55	2018-08-02 15:06:55	1	1	2.2 MB

YOU CAN WRITE YARA RULES TO AUTOMATICALLY HUNT FOR THINGS

Secure | https://www.virustotal.com/intelligence/search/?query=humoronoff.top

Search Hunting Clustering Statistics Help New joshpyorre

File information

Identification | Details | Content | Analyses | Submissions | ITW | Behaviour | Comments

Hexview | Strings

```
          00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
00000010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
00000050  69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f   is program canno
00000060  74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20   t be run in DOS 
00000070  6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00   mode....$.......
00000080  9e d1 86 0e da b0 e8 5d da b0 e8 5d da b0 e8 5d   .......]...]...]
00000090  c4 e2 7d 5d c9 b0 e8 5d c4 e2 6c 5d ea b0 e8 5d   ..}]...]..l]...]
000000A0  c4 e2 6b 5d bd b0 e8 5d fd 76 93 5d d1 b0 e8 5d   ..k]...].v.]...]
000000B0  da b0 e9 5d ab b0 e8 5d 5a fe bf b8 db b0 e8 5d   ...]...]Z......]
000000C0  c4 e2 7c 5d db b0 e8 5d a0 b3 a5 39 db b0 e8 5d   ..|]...]...9...]
000000D0  52 69 63 68 da b0 e8 5d 00 00 00 00 00 00 00 00   Rich...]........
000000E0  50 45 00 00 4c 01 05 00 7a 79 61 5b 00 00 00 00   PE..L...zya[....
000000F0  00 00 00 00 e0 00 02 01 0b 01 09 00 00 92 00 00   ................
00000100  00 3e 02 00 00 00 00 00 a1 1b 00 00 00 10 00 00   .>..............
```

Download file | Re-scan file | Close

AND YOU CAN DOWNLOAD AND PROCESS FILES, GETTING USEFUL INFO

IN ADDITION TO STATIC/HISTORICAL MALICIOUSNESS, THERE ARE LIVE FEEDS

FEEDS

Bambenek Consulting

isctdtaulbpoprun.pw

```
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
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
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
```

WHY VISUALS?

- Turn Messy Data into Meaningful Information
- Help Us Quickly Analyze Threat Hunting Data

Assessments of change, dynamics, and cause and effect are at the heart of thinking and explanation. To understand is to know…

What cause provokes what effect, by what means, at what rate.

How then is such knowledge to be represented?

~Edward Tufte

VISUALS THAT WE LIKE TO USE

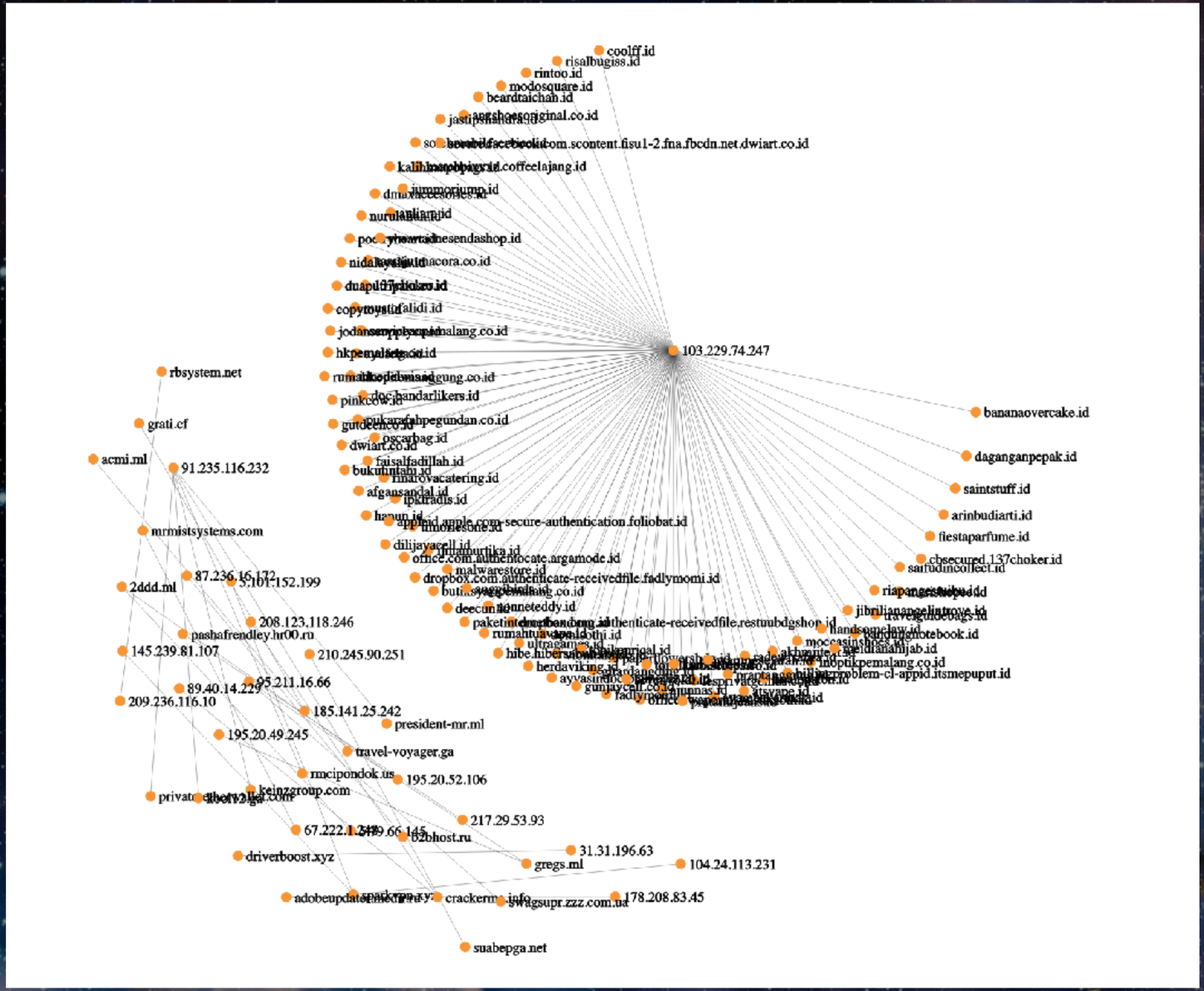
Data-Driven Documents

WE PROCESS WITH PYTHON AND THEN VISUALIZE USING D3 AND MATPLOTLIB

VISUALS WE LIKE TO USE

- Force-Directed Graph
- Timelines of First Seen Queries VS Domain Registration
- Timelines of Domain Queries
- Timelines of Queries From Network Captures
- Signature Patterns Built From Queries In Network Capture Files

FORCE-DIRECTED GRAPHS



View On GitHub

OpenGraphiti

OpenDNS Data Visualization Framework

Project maintained by Thibault Reuille

Powered by OpenDNS

Description

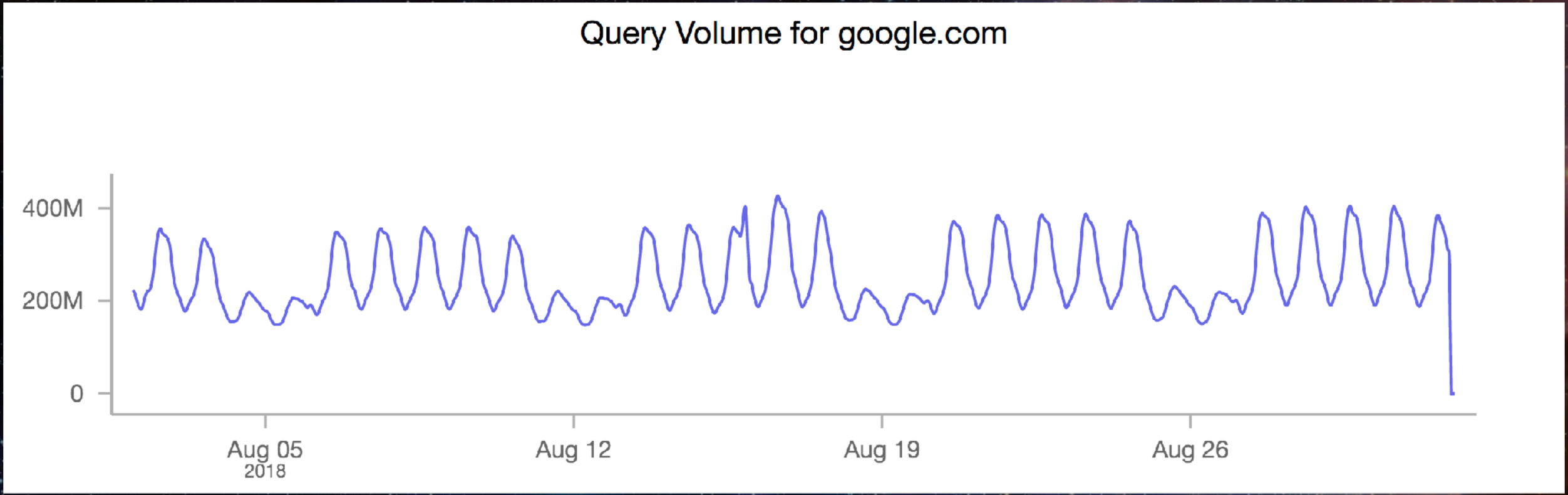
OpenGraphiti is a free and open source 3D data visualization engine for data scientists to visualize semantic networks and to work with them. It offers an easy-to-use API with several associated

SOME OF THE BEAUTIFUL THINGS YOU CAN CREATE WITH FORCE-DIRECTED GRAPHS

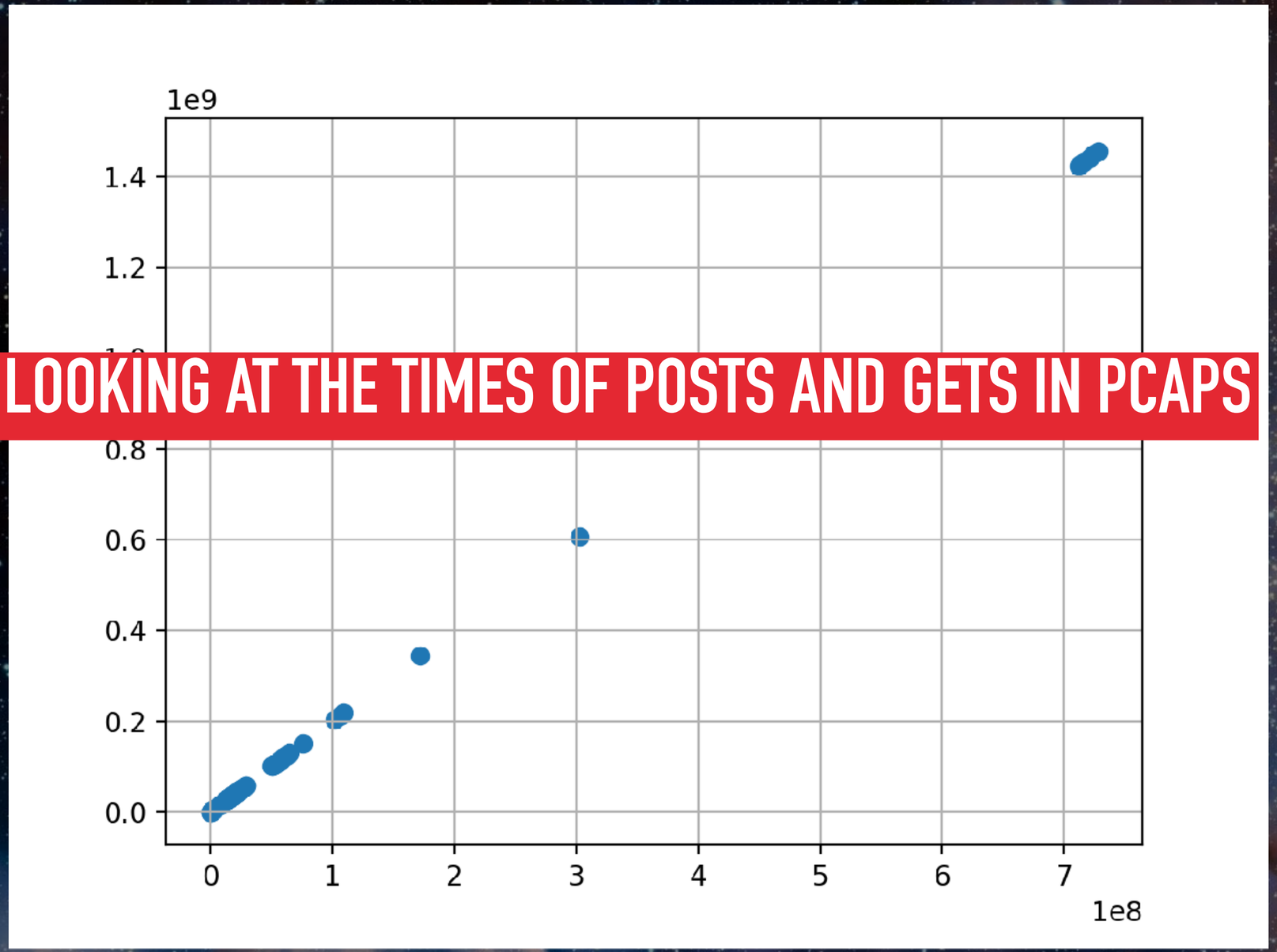
GAMEOVER ZEUS

MIRAI
Mirai

QUERY TIMELINES



PATTERN MATCHING

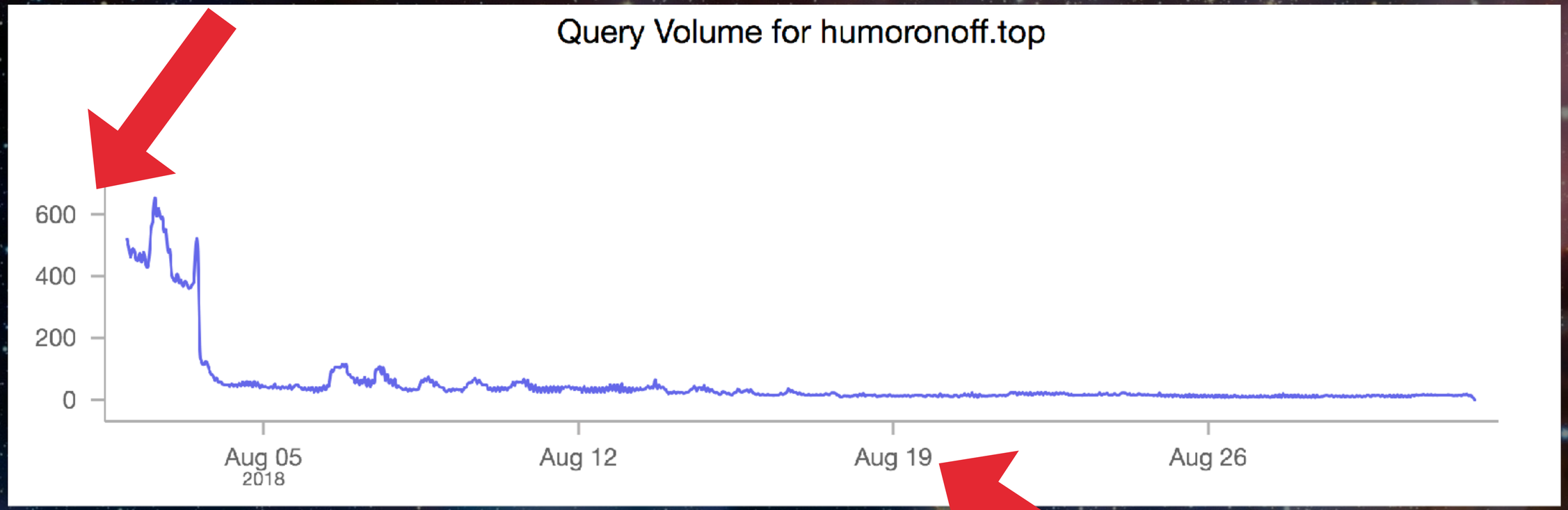


LOOKING AT THE TIMES OF POSTS AND GETS IN PCAPS

WHAT MAKES A VISUAL USEFUL?

QUESTIONS WE ASK OURSELVES

When showing quantities, what will make the visual clear?



QUESTIONS WE ASK OURSELVES

Am I placing the data in an appropriate context?

force directed graphs: intuitive for networks

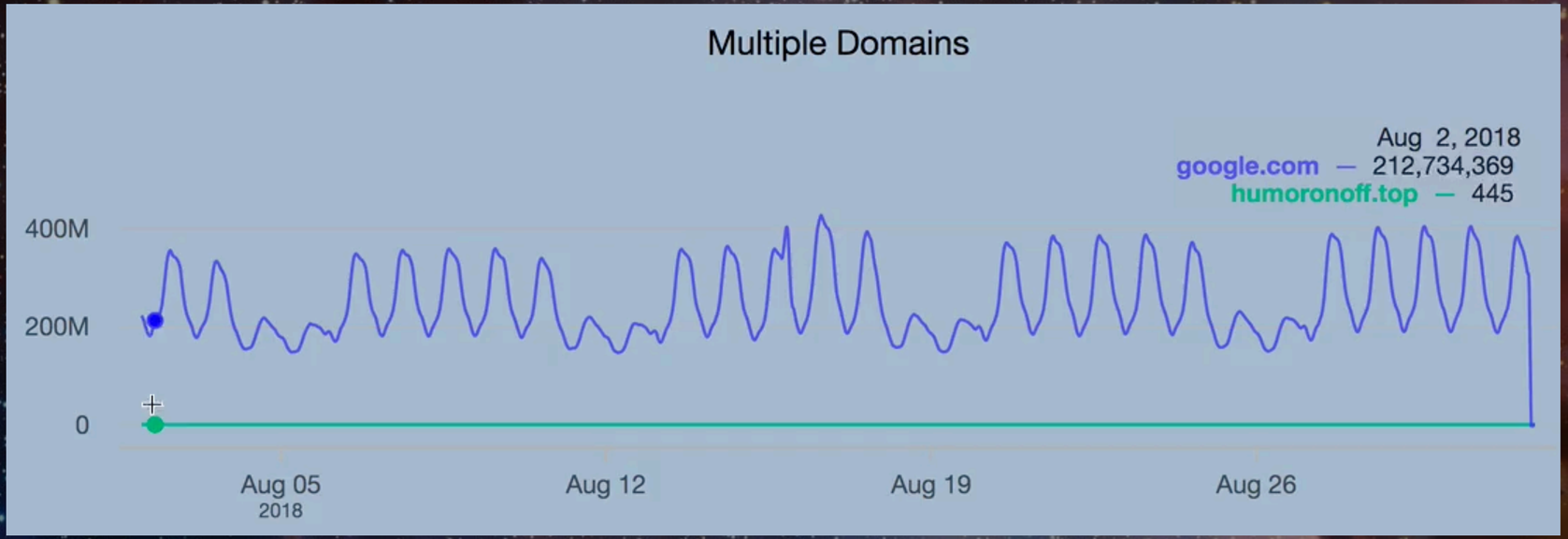
QUESTIONS WE ASK OURSELVES

How can I ...

. reduce visual clutter ?

. clarify primary information ?

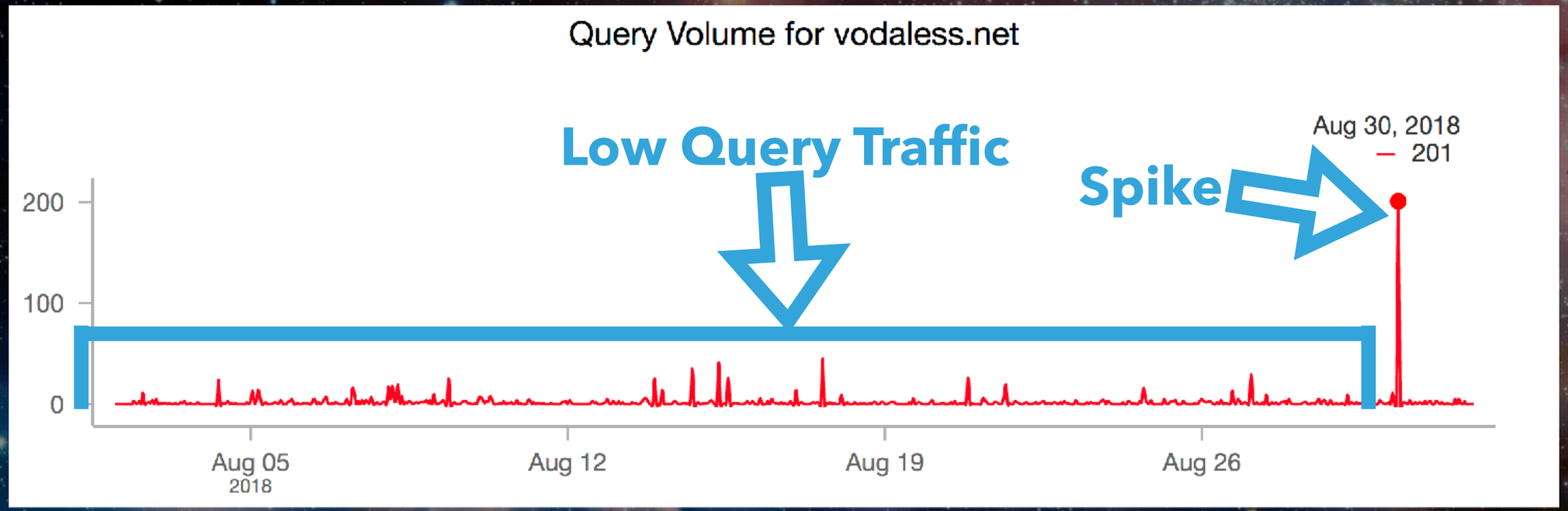
. highlight notable content ?



QUESTIONS WE ASK OURSELVES

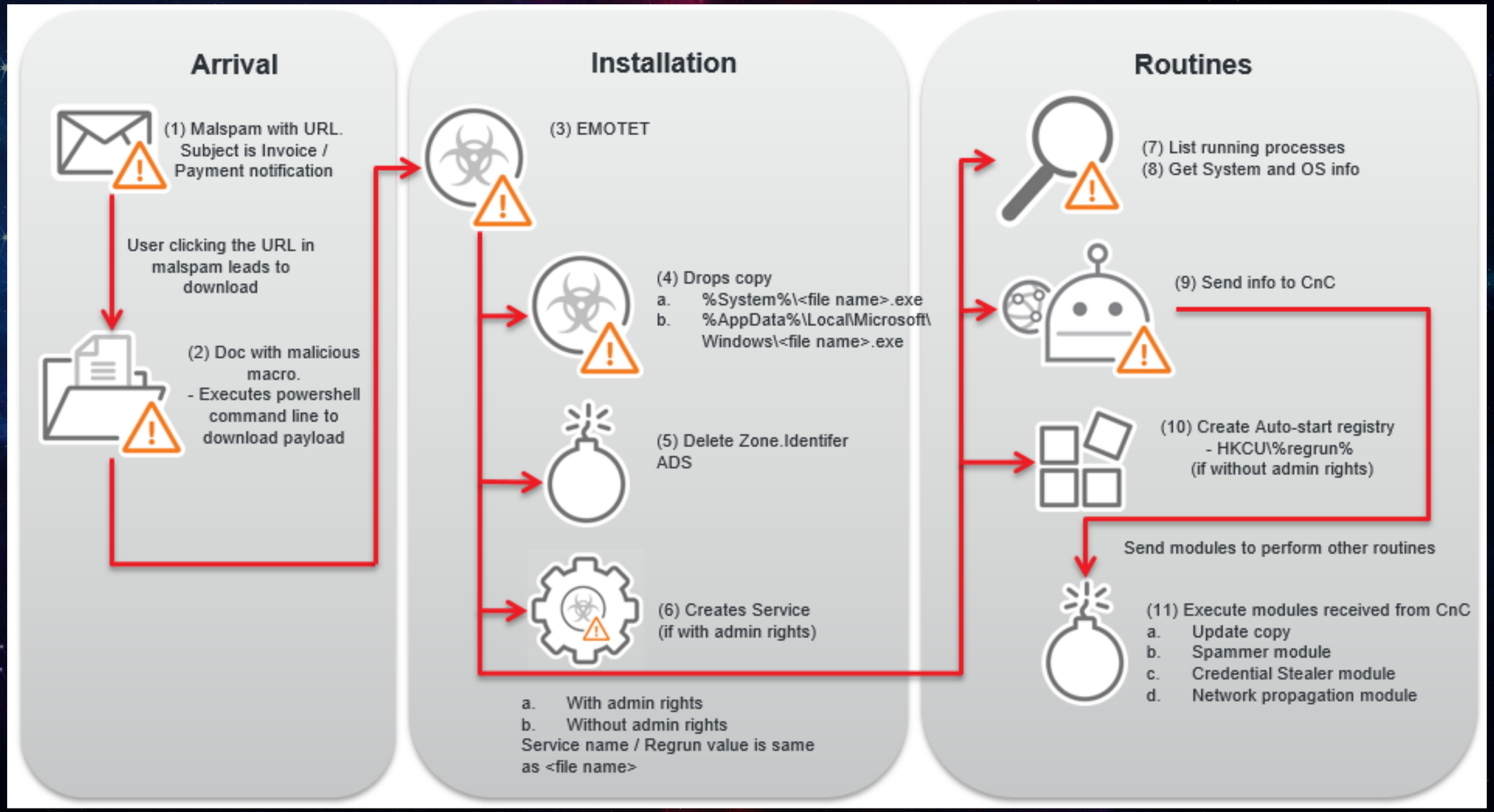
How can I assess change and rates of change ?

- Queries on Different Days to Same Domain Reveal Patterns, Assessed Change, and Rates of Change.
- We See This On Domains Which Show a Sudden Spike (the assessed change) and How Many Queries There Were On The Spike (or if it ever happened)



VISUAL EXAMPLES OF ATTACK CAMPAIGNS

EMOTET


Arrival
(1) Malspam with URL. Subject is Invoice / Payment notification
User clicking the URL in malspam leads to download
(2) Doc with malicious macro.
- Executes powershell command line to download payload
Installation
(3) EMOTET
(4) Drops copy
a. %System%\<file name>.exe
b. %AppData%\Local\Microsoft\Windows\<file name>.exe
(5) Delete Zone.Identifer ADS
(6) Creates Service (if with admin rights)
a. With admin rights
b. Without admin rights
Service name / Regrun value is same as <file name>
Routines
(7) List running processes
(8) Get System and OS info
(9) Send info to CnC
(10) Create Auto-start registry
- HKCU\%regrun%
(if without admin rights)
Send modules to perform other routines
(11) Execute modules received from CnC
a. Update copy
b. Spammer module
c. Credential Stealer module
d. Network propagation module

FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

Emotet_domains.txt

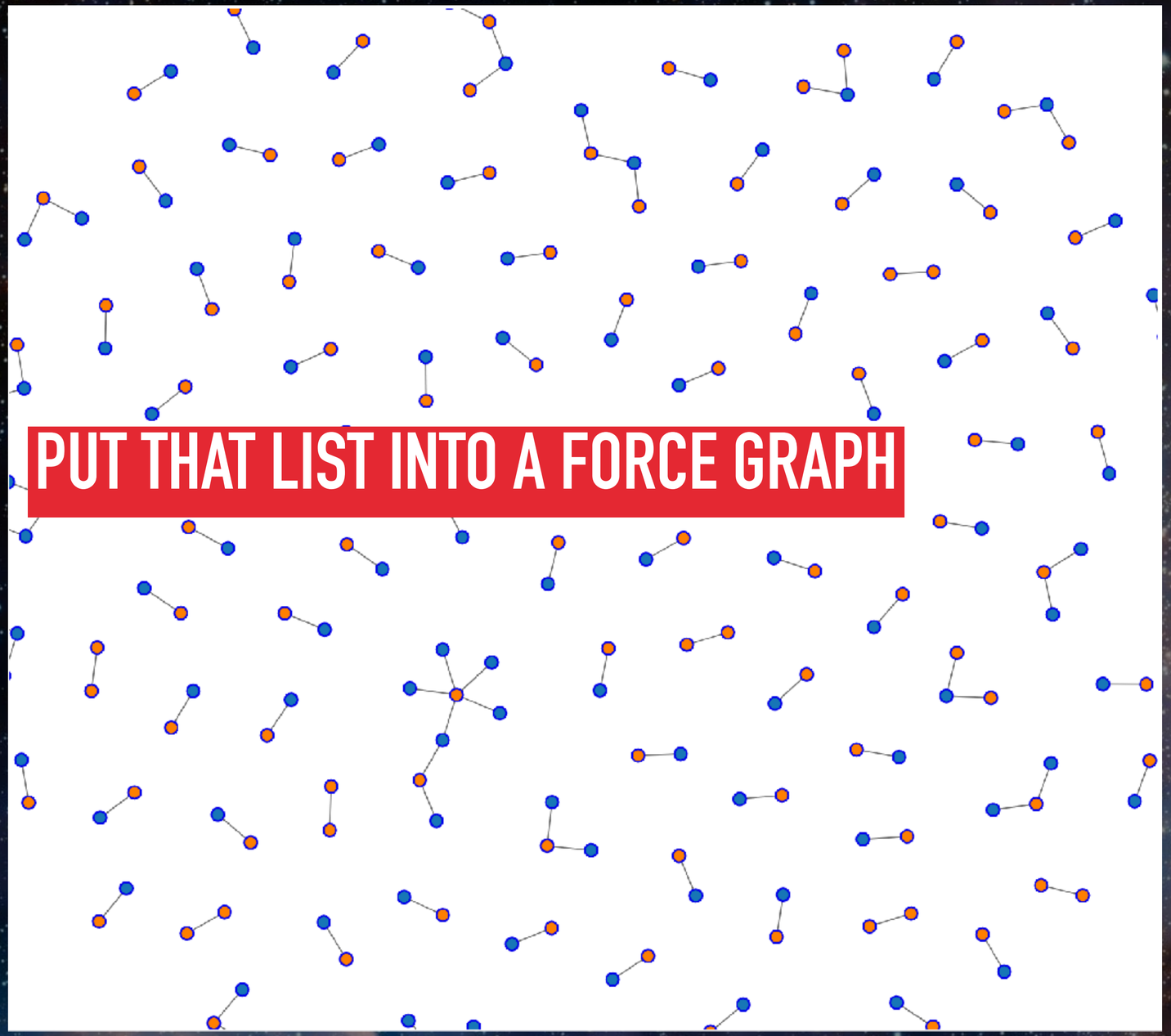
```
atakentegitimkurumlari.com
gadanie-lidia.ru
vodaless.net
eclatpro.com
weliketomoveit.ca
fundacionafanic.com
eeodlewnia.pl
simcon.ca
ownhive.com
gnatyshyn.pl
soportek.cl
ipinfo.io
goprorent.pl
irontech.com.tr
msftncsi.com
krufgqsp.com
collectorsway.com
webmounts.co.ke
brokbutcher.com
ocyoungactors.com
misico.com
```

Emotet_ips.txt

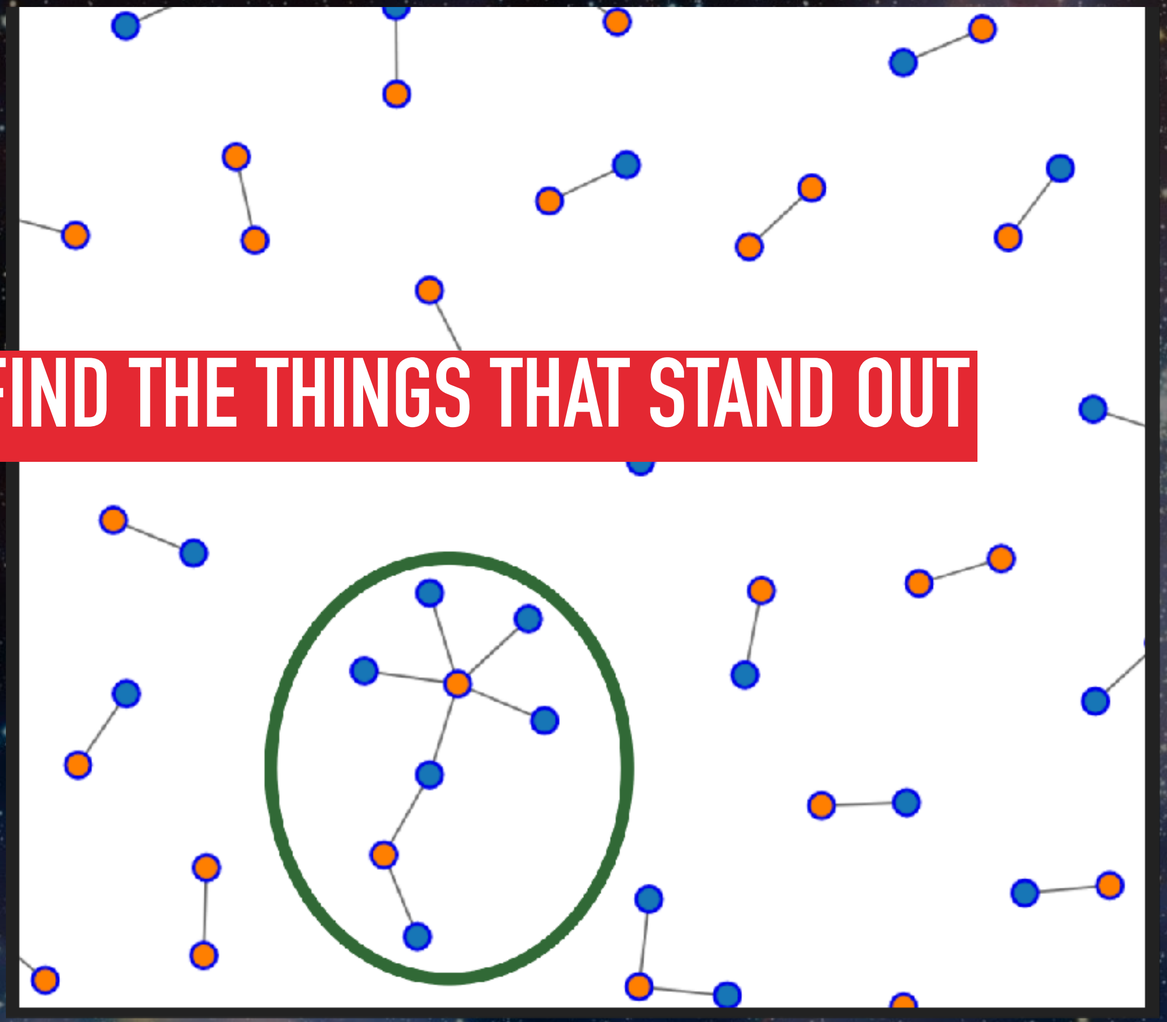
```
12.182.146.226
186.71.61.91
181.142.74.233
71.202.205.235
185.159.131.55
37.120.175.15
69.17.170.58
24.217.117.217
79.78.160.225
73.178.169.180
129.89.95.241
73.27.38.128
129.89.95.110
96.95.159.237
24.40.239.62
71.8.1.188
71.71.3.84
199.120.92.245
186.71.61.91
181.142.74.233
71.202.205.235
```

OFTEN, YOU JUST HAVE A LISTS OF DOMAINS AND IPS

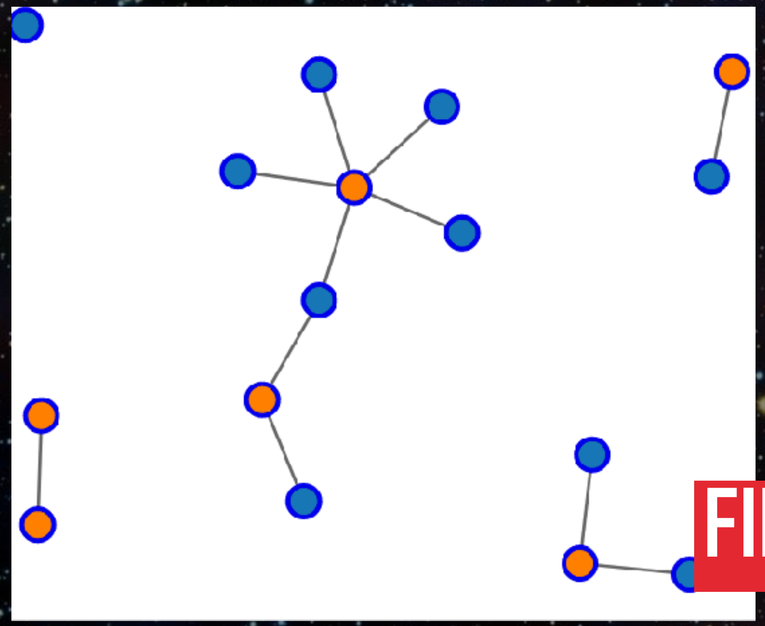
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

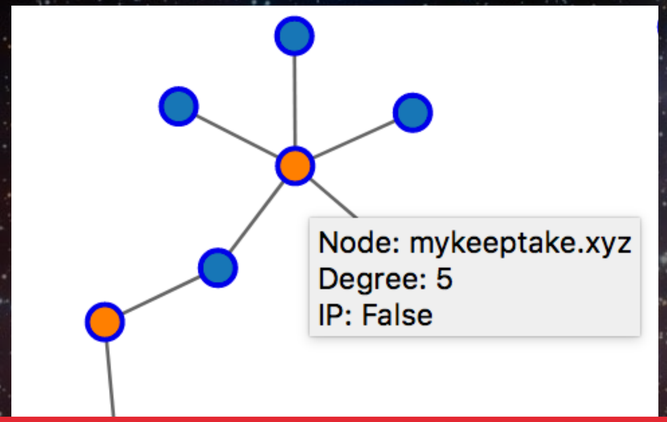


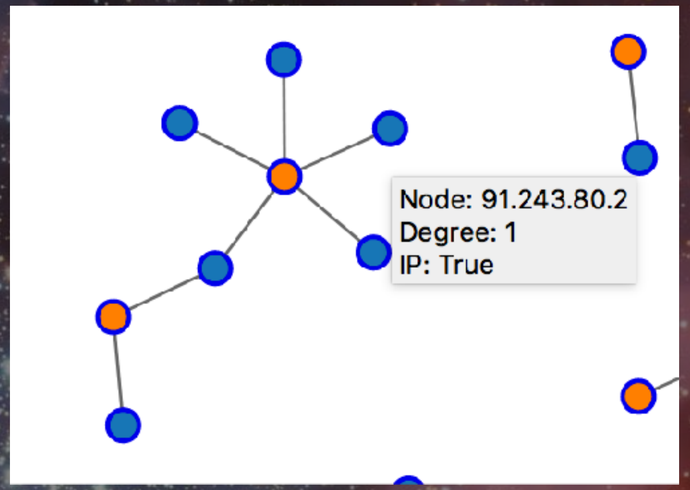
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS



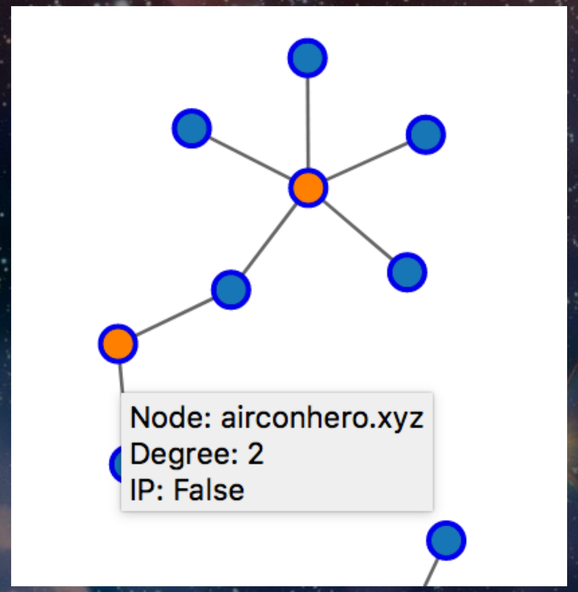
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

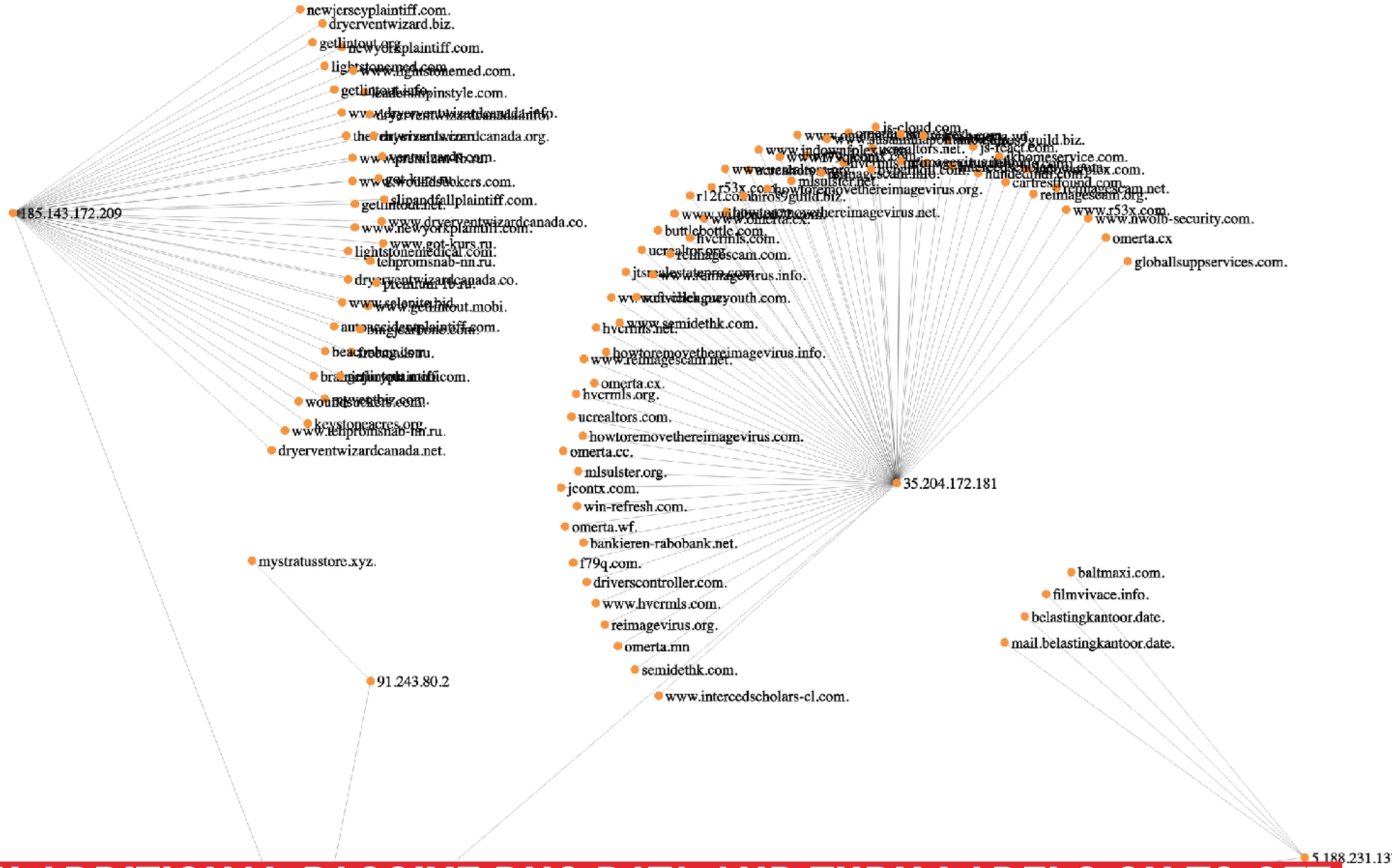






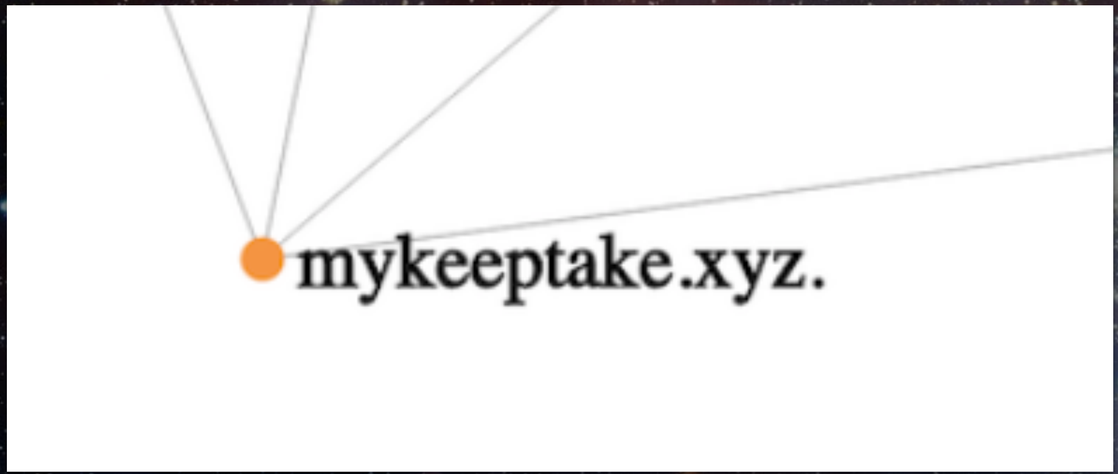
FIND THE THINGS THAT STAND OUT





ENRICH THAT WITH ADDITIONAL PASSIVE DNS DATA AND TURN LABELS ON TO GET MORE INFO

THIS DOMAIN, ASSOCIATED WITH EMOTET WILL BE SEEN AGAIN LATER



TIMELINES

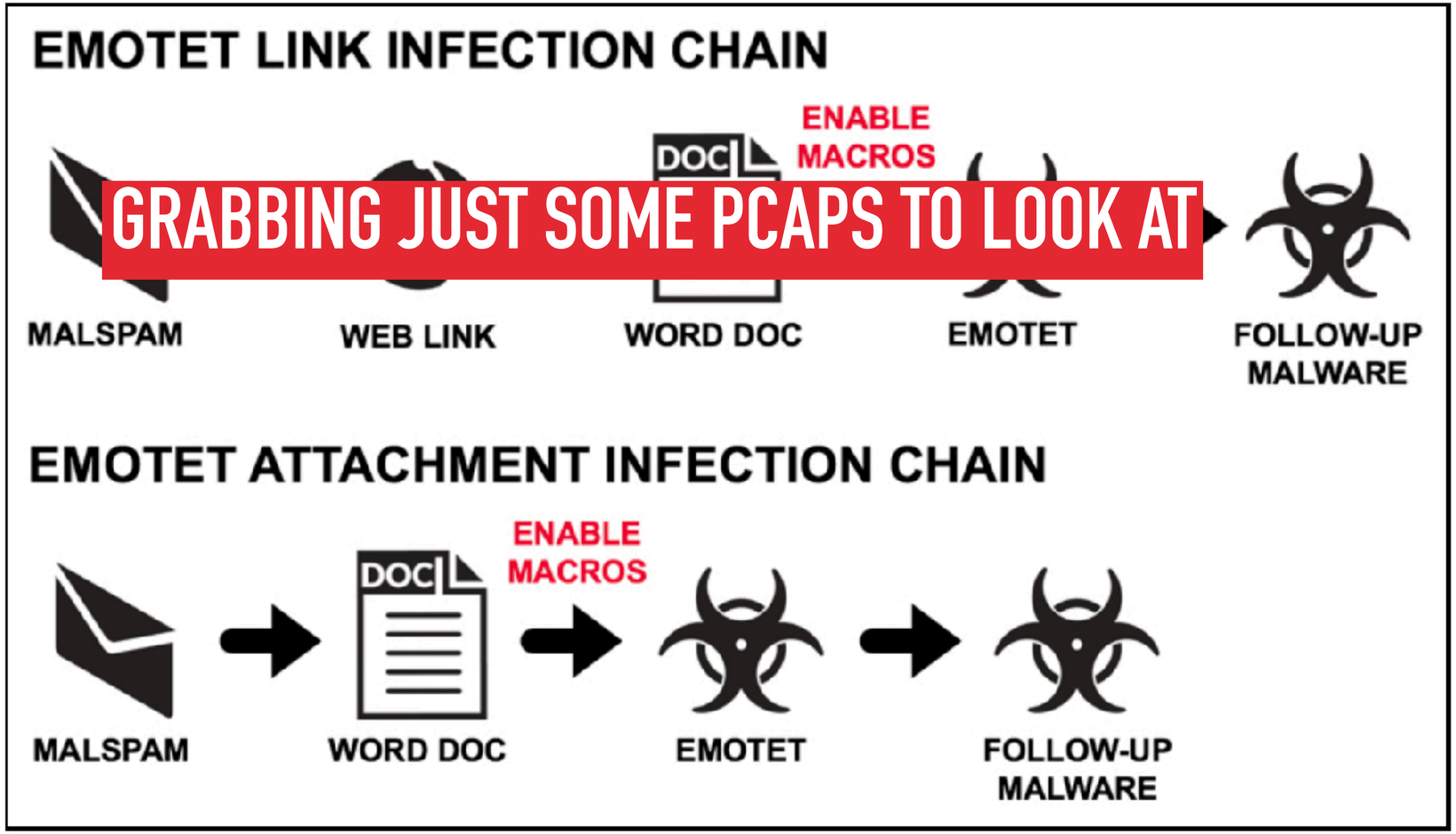
2018-08-16 - EMOTET INFECTIONS WITH ZEUS PANDA BANKER ON 2018-08-15 & 2018-08-16

ASSOCIATED FILES:

- **2018-08-14-thru-16-Emotet-malspam-9-email-examples.zip** 420 kB (420,083 bytes)
- **2018-08-15-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 1.4 MB (1,352,380 bytes)
- **2018-08-16-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip** 4.2 MB (4,225,183 bytes)
- **2018-08-14-thru-16-malware-associated-with-Emotet-infections.zip** 1.2 MB (1,132,372 bytes)

NOTES:

- Still seeing Zeus Panda Banker caused by Emotet, very similar to what I posted earlier this week on **2018-08-14**.
- This ties into a recent Unit 42 blog I wrote last month, **Malware Team Up: Malspam Pushing Emotet + Trickbot**.



GRABBING JUST SOME PCAPS TO LOOK AT

Shown above: Flow chart typical Emotet malspam infections.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.546015	10.8.15.103	195.162.24.96	HTTP	354	GET /WellsFargo/Smallbusiness/Aug-15-2018 HTTP/1.1
8	0.760924	195.162.24.96	10.8.15.103	HTTP	615	HTTP/1.1 301 Moved Permanently (text/html)
10	0.769095	10.8.15.103	195.162.24.96	HTTP	355	GET /WellsFargo/Smallbusiness/Aug-15-2018/ HTTP/1.1
205	1.529418	195.162.24.96	10.8.15.103	HTTP	1231	HTTP/1.1 200 OK (application/msword)
216	27.170271	10.8.15.103	201.148.107.187	HTTP	122	GET /FAm4eZY HTTP/1.1
218	27.474371	201.148.107.187	10.8.15.103	HTTP	537	HTTP/1.1 301 Moved Permanently (text/html)
219	27.478109	10.8.15.103	201.148.107.187	HTTP	99	GET /FAm4eZY/ HTTP/1.1
413	29.410187	201.148.107.187	10.8.15.103	HTTP	236	HTTP/1.1 200 OK (application/octet-stream)
424	99.976226	10.8.15.103	93.88.93.99	HTTP	828	GET / HTTP/1.1
426	100.770968	93.88.93.99	10.8.15.103	HTTP	342	HTTP/1.1 200 OK (text/html)
430	160.008743	10.8.15.103	93.88.93.99	HTTP	828	GET / HTTP/1.1

```
GET /WellsFargo/Smallbusiness/Aug-15-2018 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: akademia.gnatyshyn.pl
DNT: 1
Connection: Keep-Alive
```

No.	Time	Source	Destination	Protocol	Length	Info
213	26.840344	10.8.15.103	201.148.107.187	TCP	66	49205 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
214	27.169656	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
215	27.169859	10.8.15.103	201.148.107.187	TCP	60	49205 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
216	27.170271	10.8.15.103	201.148.107.187	HTTP	122	GET /FAm4eZY HTTP/1.1
217	27.170273	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [ACK] Seq=1 Ack=69 Win=64240 Len=0
218	27.474371	201.148.107.187	10.8.15.103	HTTP	537	HTTP/1.1 301 Moved Permanently (text/html)
219	27.478109	10.8.15.103	201.148.107.187	HTTP	99	GET /FAm4eZY/ HTTP/1.1
220	27.478110	201.148.107.187	10.8.15.103	TCP	60	80 → 49205 [ACK] Seq=484 Ack=114 Win=64240 Len=0
221	27.781664	201.148.107.187	10.8.15.103	TCP	478	80 → 49205 [PSH, ACK] Seq=484 Ack=114 Win=64240 Len=424 [TCP seg
222	27.781668	201.148.107.187	10.8.15.103	TCP	1399	80 → 49205 [PSH, ACK] Seq=908 Ack=114 Win=64240 Len=1345 [TCP se
223	27.782093	10.8.15.103	201.148.107.187	TCP	60	49205 → 80 [ACK] Seq=114 Ack=2253 Win=64240 Len=0

```
GET /FAm4eZY HTTP/1.1
Host: soportek.cl
Connection: Keep-Alive
```

2. bash

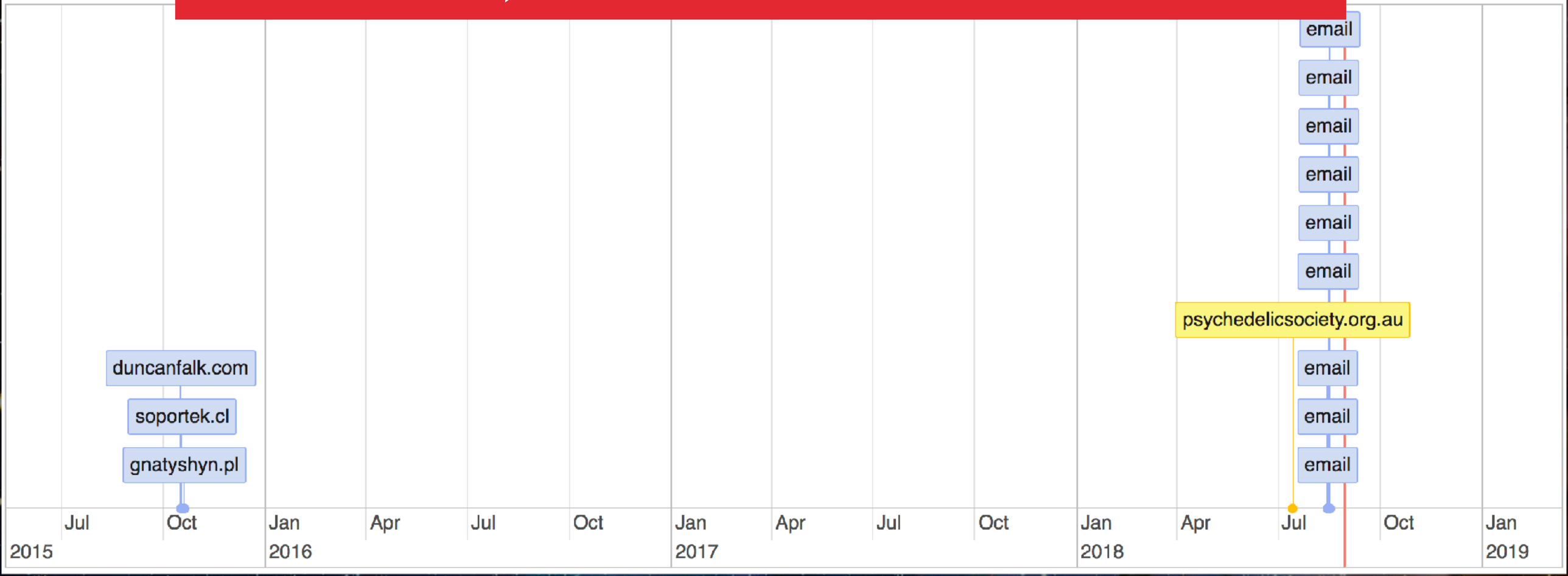
```
python process_pcap.py 2018-08-15-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap
```

```
duncanfalk.com
psychedelicsociety.org.au
gnatyshyn.pl
soportek.cl
```

PULL OUT THE DOMAINS WITH PYTHON

FROM ONE NETWORK CAPTURE

BUILD A TIMELINE, SHOWING THE TIMES EMAILS WERE RECEIVED



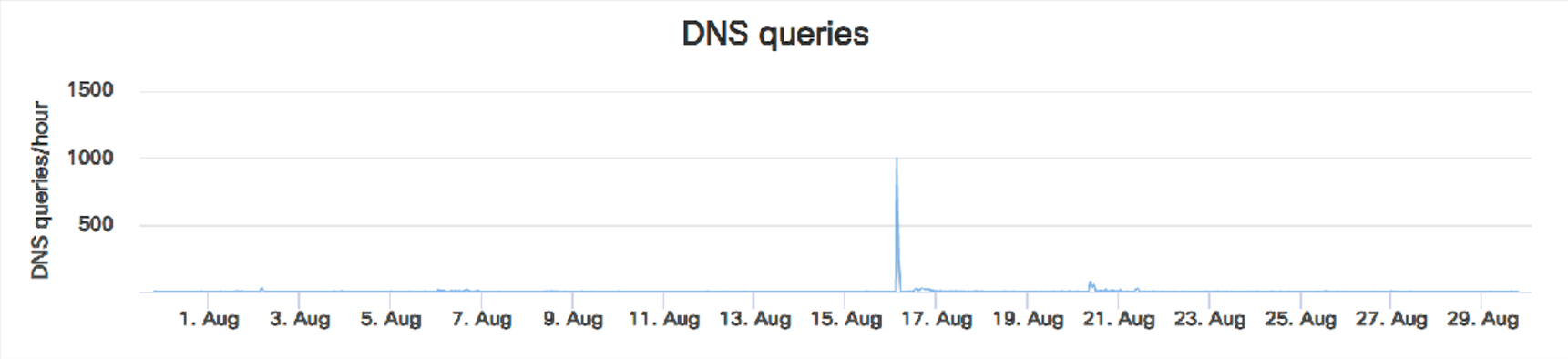
AND WHEN DOMAINS WERE FIRST-SEEN IN DNS

Details for psychedelicsociety.org.au

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 45

This domain is associated with a Trojan attack called Emotet



Current Status

First Seen	2018/07/14 10:19
First Queried	2018/07/14 10:19
Categories	Malware
Attacks	Emotet
Threat Types	Trojan

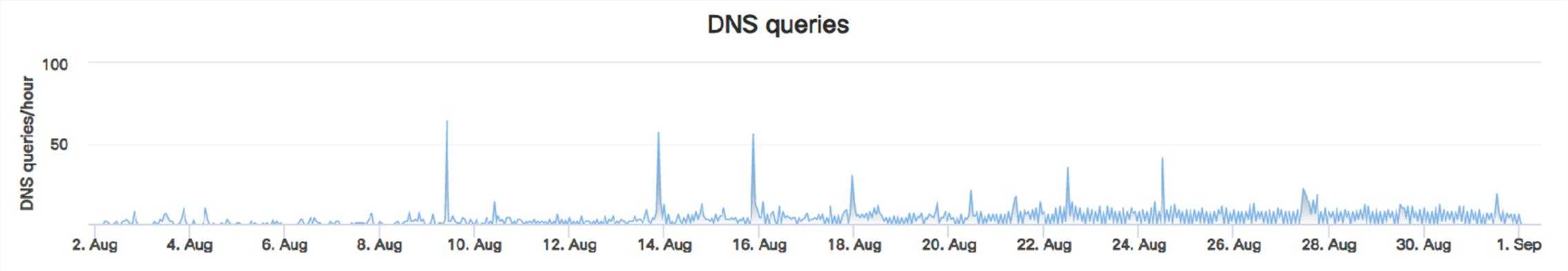
LOOKING AT INFORMATION ON THE DOMAINS IN THOSE PCAPS

Details for duncanfalk.com

This domain is currently in the Umbrella block list

Umbrella Investigate Risk Score: 60

This domain is associated with a Trojan attack called Emotet



Current Status

First Seen	2015/10/16 14:51
First Queried	2016/09/19 04:39
Categories	Malware
Attacks	
Threat Types	Trojan

LOOKING AT INFORMATION ON THE DOMAINS IN THOSE PCAPS

Latest URLs hosted in this domain **detected by at least one URL scanner or malicious URL dataset.**

7/68	2018-08-27 19:49:33	http://psychedelicsociety.org.au/wp-content/plugins/woocommerce/includes/ce8bGv.html
8/68	2018-08-23 20:12:54	http://psychedelicsociety.org.au/
7/68	2018-08-22 05:55:13	http://psychedelicsociety.org.au/ek8jzyn/qwedlue.php
10/69	2018-08-19 05:38:51	http://psychedelicsociety.org.au/3mw
8/70	2018-08-17 18:24:57	https://psychedelicsociety.org.au/3mw
1/68	2018-08-10 04:49:12	http://psychedelicsociety.org.au/wp-content/uploads/2018/07/no5pd4.php

LOOKING AT INFORMATION ON THE DOMAINS IN THOSE PCAPS

www.psychedelicsociety.org.au

Search

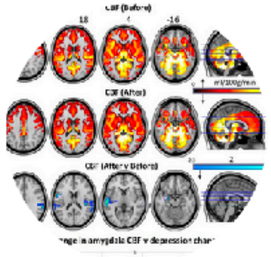
Australian Psychedelic Society

News Events Knowledge Newsletter Contact

The Australian Psychedelic Society is an organisation seeking to connect Australia's psychedelic community to benefit, enjoy and contribute to their culture in a safe and supportive environment.

Upcoming Events

Become a member



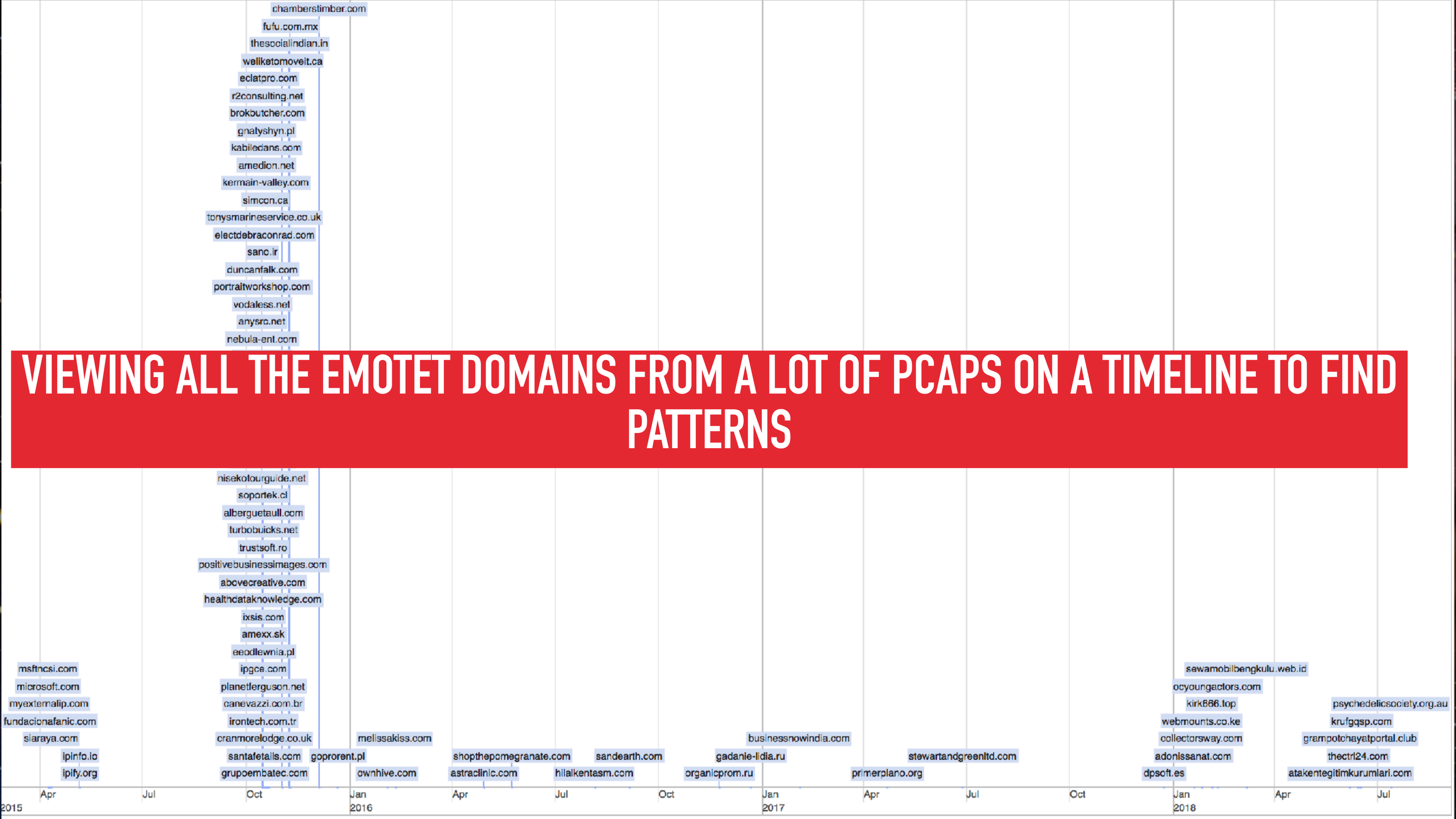
APS News

ACTUALLY VISITING THE DOMAIN, A COMPROMISED INSTANCE OF WORDPRESS

Advocate: For the interests of the psychedelic community.

Represent: Provide an informed and balanced public voice for the psychedelic community

VIEWING ALL THE EMOTET DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS



PATTERNS

LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 2018-06-05-Emotet-malspam-infection-traffic.pcap

```
GET /ups.com/WebTracking/PX-5748789735663/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.pod.siaraya.com
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 05 Jun 2018 17:52:53 GMT
Server: Apache
X-Powered-By: PHP/5.3.29
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Disposition: attachment; filename="2TX53437800424385.doc"
Content-Transfer-Encoding: binary
Keep-Aliv
Connectio
Transfer-
Content-T

19800
.......................>.....
................V...........Y...............U.......................................................................
.....................................................................................................................
.....................................................................................................................
.....................................................................................................................
.....................................;.  ........................bjbj%.%.................
.......G..dG..d.....................................................................................................
+.......+.......+.......+.......
+......................?.......?.......?.......?.......K.......?...............W.......W.......W.......W.......
```

3 client pkts, 67 server pkts, 3 turns.

Entire conversation (105 kB) | Show and save data as ASCII | Stream 0

Find: | Find Next

Help | Filter Out This Stream | Print | Save as... | Back | Close

2018-06-05-Emotet-malspam-infection-traffic.pcap

ttp

	Time	Source	Destination	Protocol	Length	Info
6	0.438379	10.6.5.102	103.18.246.76	HTTP	353	GET /ups.com/WebTracking/PX-5748789735663/ HTTP/1.1
135	0.901247	103.18.246.76	10.6.5.102	HTTP	2885	HTTP/1.1 200 OK (application/msword)
146	30.739410					
304	31.536961					
311	48.066116					
378	63.733795	10.6.5.102	217.160.20.223	HTTP	733	POST / HTTP/1.1
1506	428.766096	217.160.20.223	10.6.5.102	HTTP	1053	HTTP/1.1 200 OK (text/html)
1514	429.262788	10.6.5.102	138.68.13.161	HTTP	325	GET /whoami.php HTTP/1.1
1516	429.760982	138.68.13.161	10.6.5.102	HTTP	224	HTTP/1.1 200 OK (text/html)
1526	433.928710	10.6.5.102	138.68.13.161	HTTP	525	POST / HTTP/1.1
1528	434.556482	138.68.13.161	10.6.5.102	HTTP	358	HTTP/1.1 200 OK (text/html)

LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

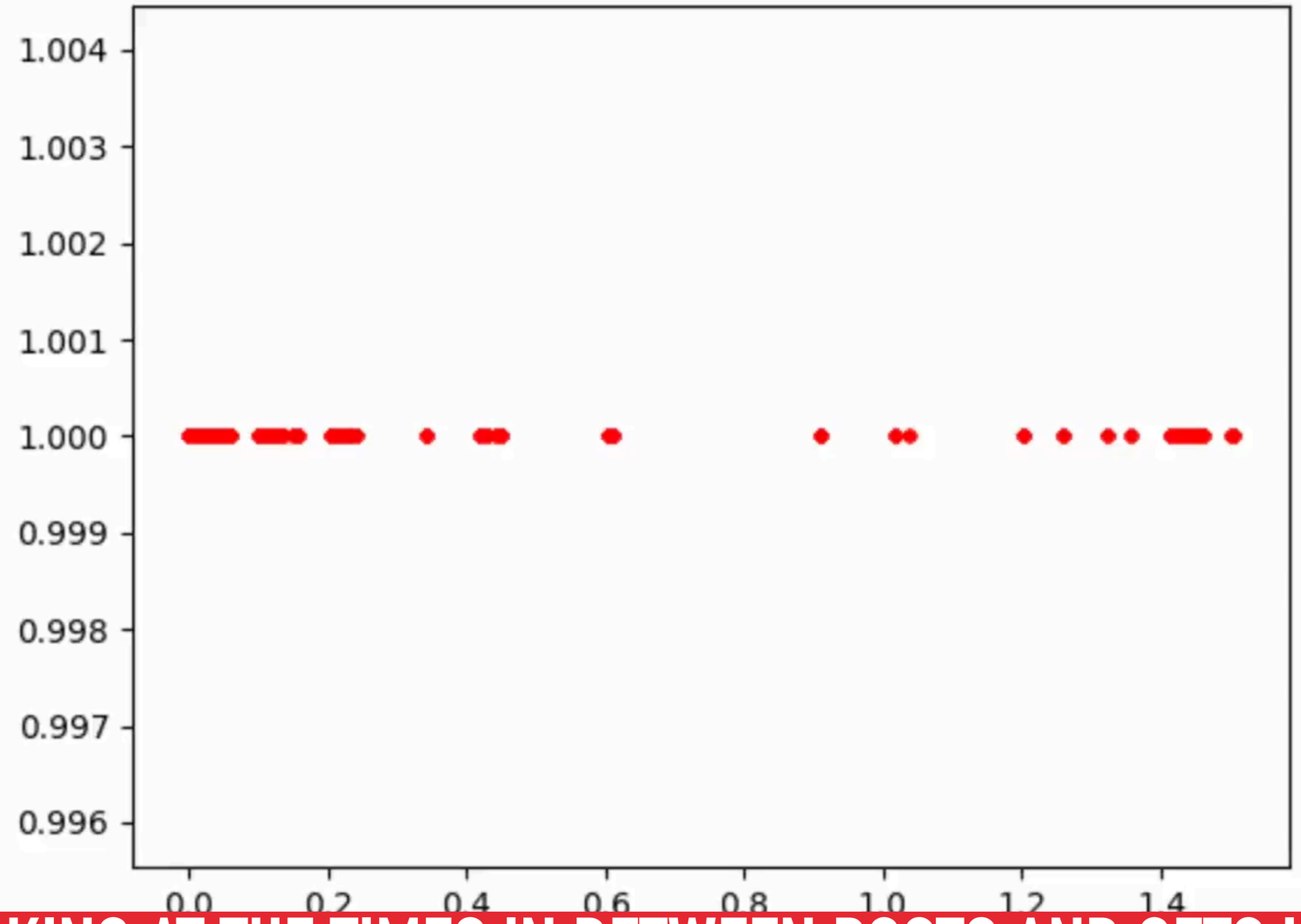
```
josh's MacBook Pro:pcap josh$ python process_pcap.py 2018-08-09-Emotet-malspam-infection-traffic.pcap
##################################################
In process_pcap():
Domains:

techwide
siaraya.com
*******************
IP's:
65.41.38.155
184.186.78.177
                                    ##########################
0:00:47.627737
0:00:15.667679
0:06:05.528993
0:00:04.665922
0:00:02.657943
0:00:29.148178
0:14:55.826192
0:14:26.409612
0:00:29.524945
0:00:00.192444
0:01:15.232961
0:00:48.174649
0:00:32.620427
0:01:25.582902
0:00:35.426778
0:00:38.802216
0:00:29.088956
```

Times In Between Events

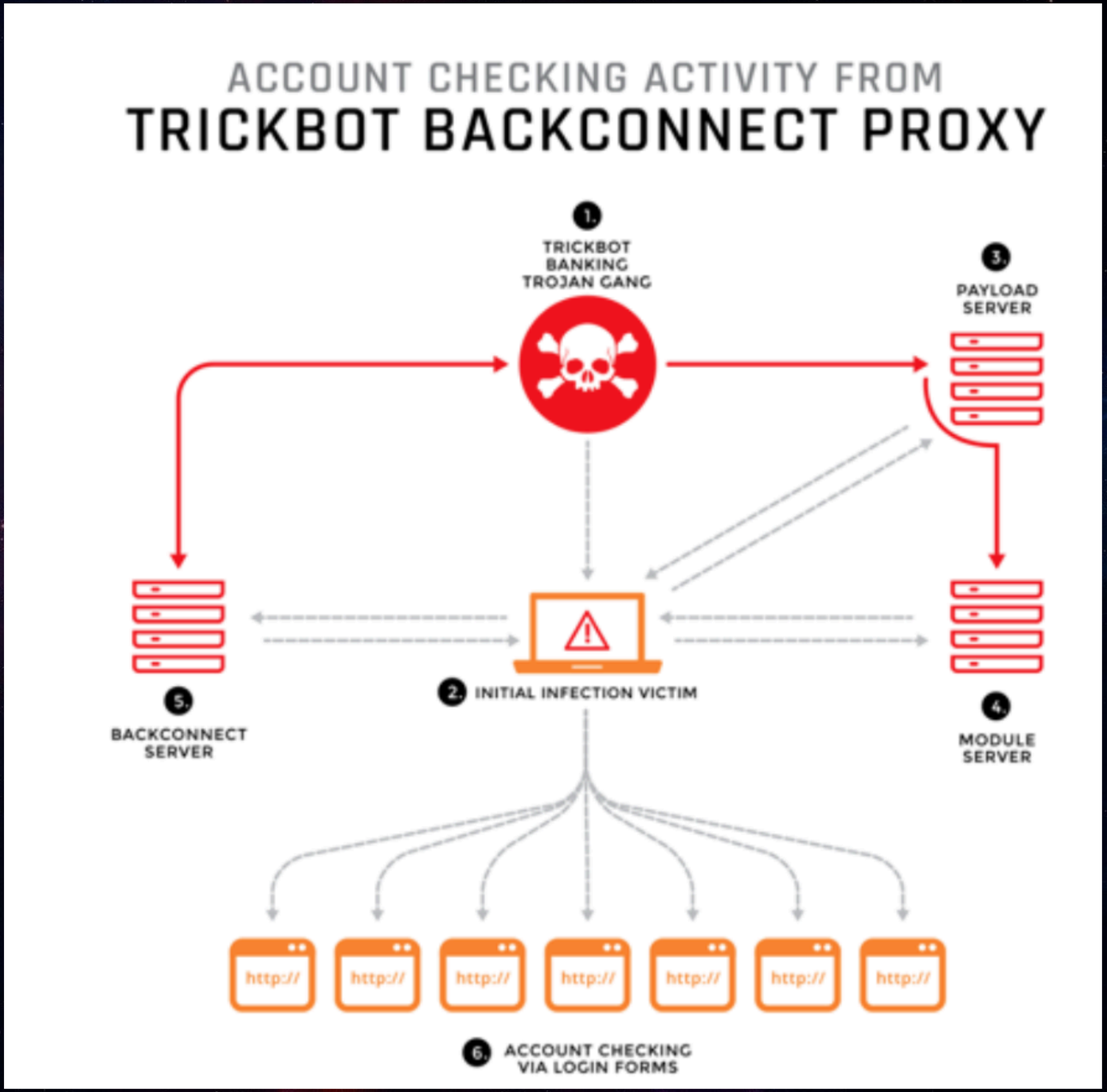
Are there patterns?

2018-06-05-Emotet-malspam-infection-traffi.png Open with Preview

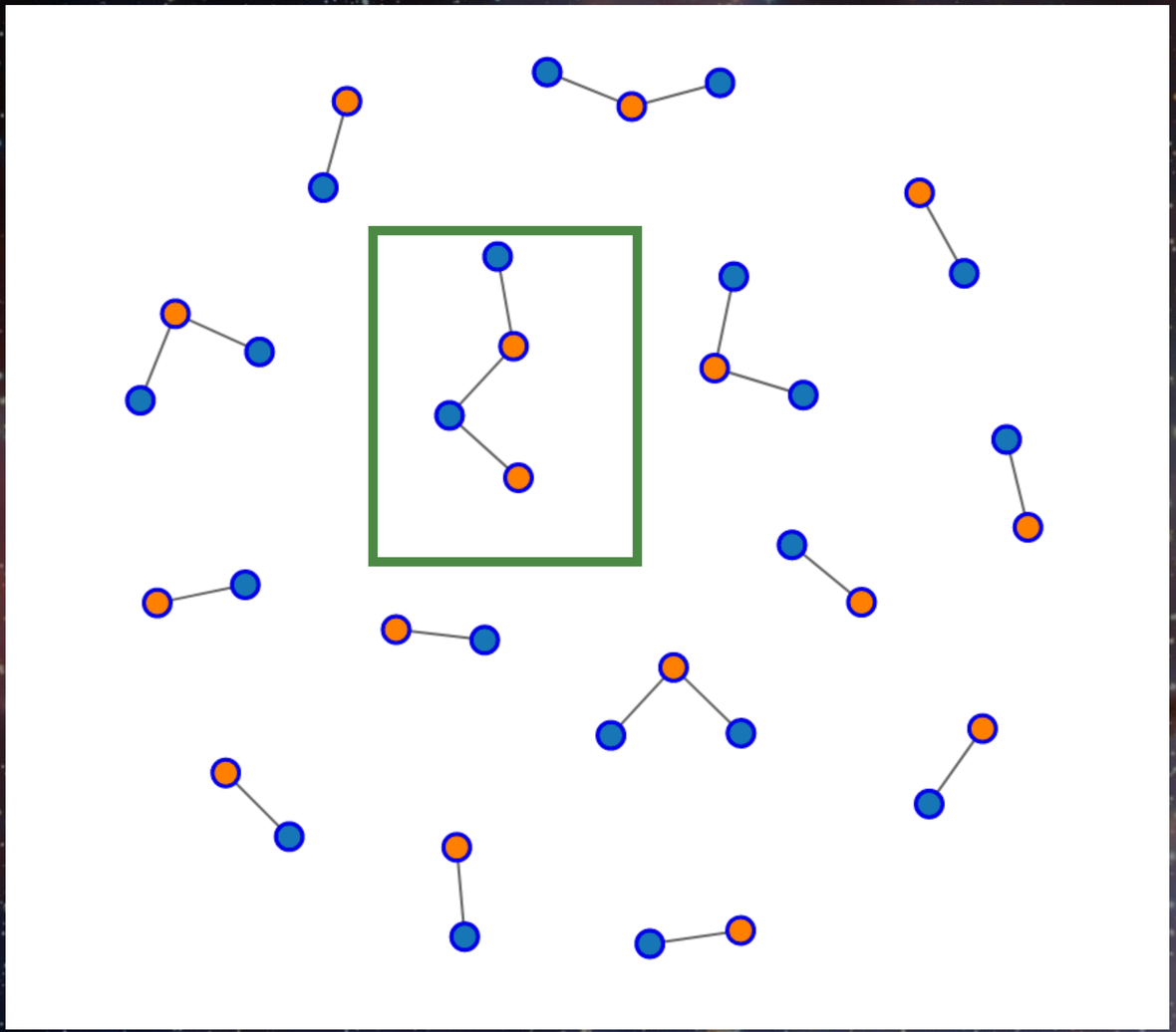


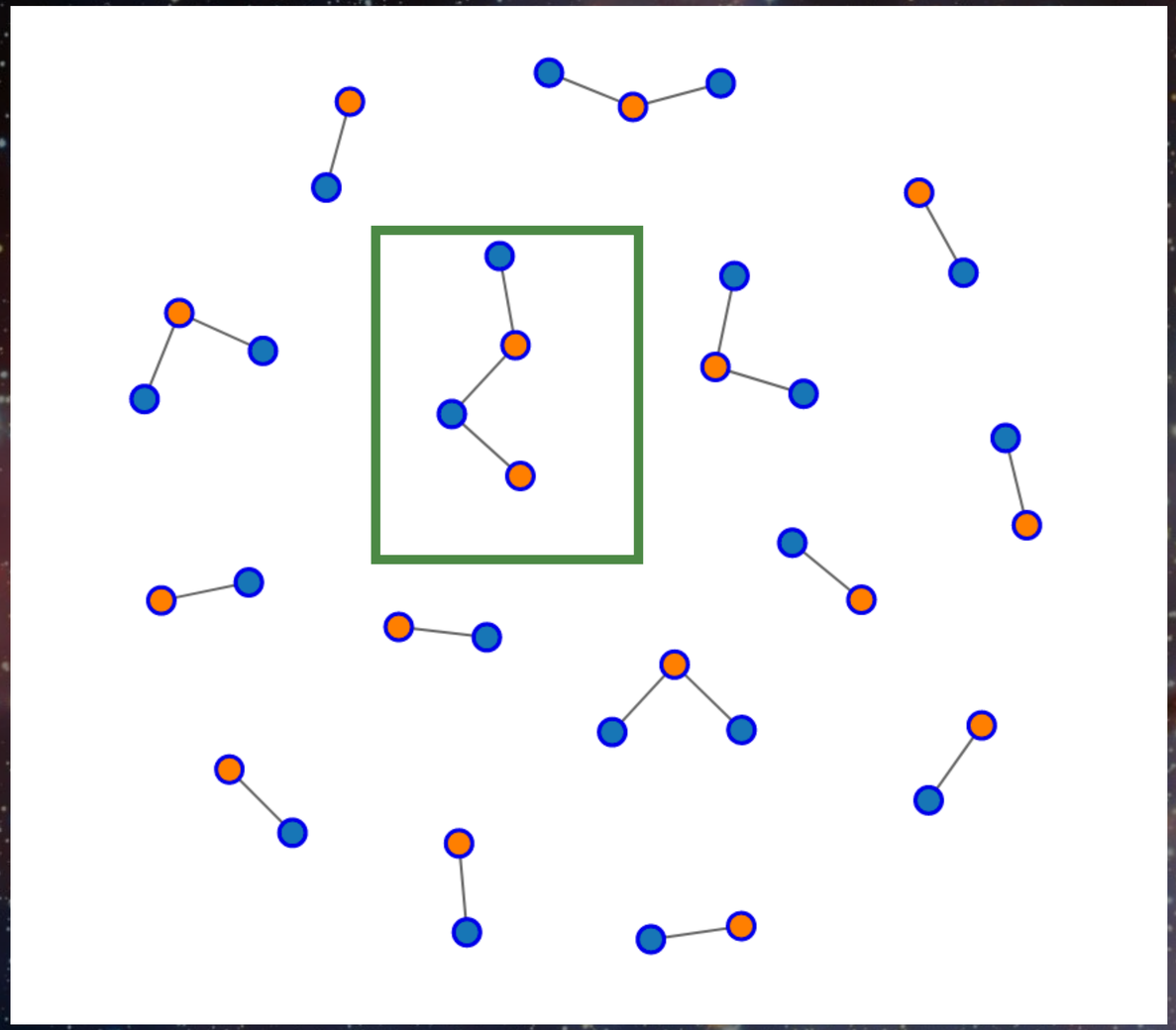
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

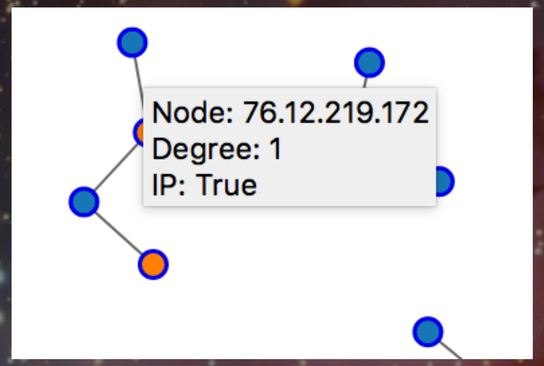
TRICKBOT

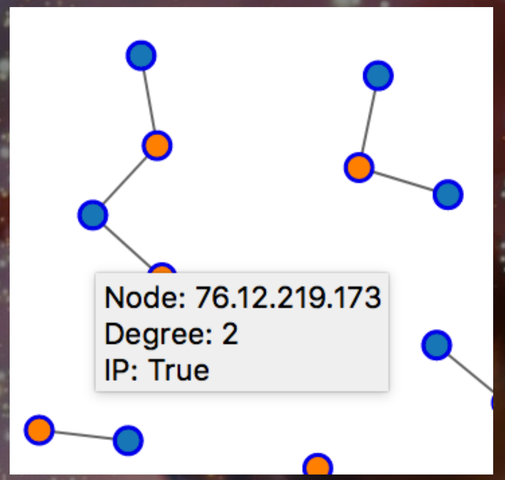

ACCOUNT CHECKING ACTIVITY FROM
TRICKBOT BACKCONNECT PROXY
1. TRICKBOT BANKING TROJAN GANG
3. PAYLOAD SERVER
5. BACKCONNECT SERVER
2. INITIAL INFECTION VICTIM
4. MODULE SERVER
http://
http://
http://
http://
http://
http://
http://
6. ACCOUNT CHECKING VIA LOGIN FORMS

GRAPHS

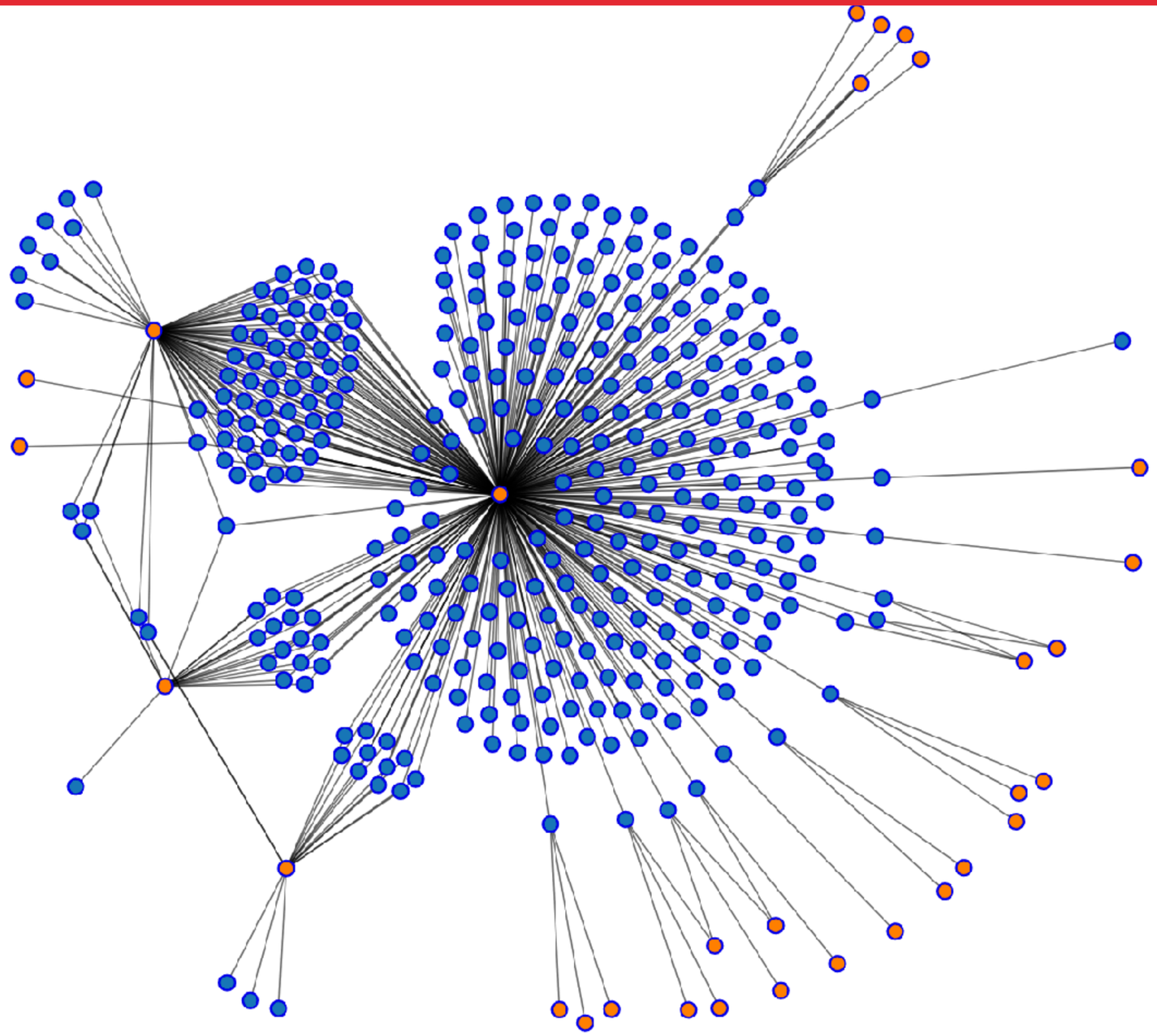




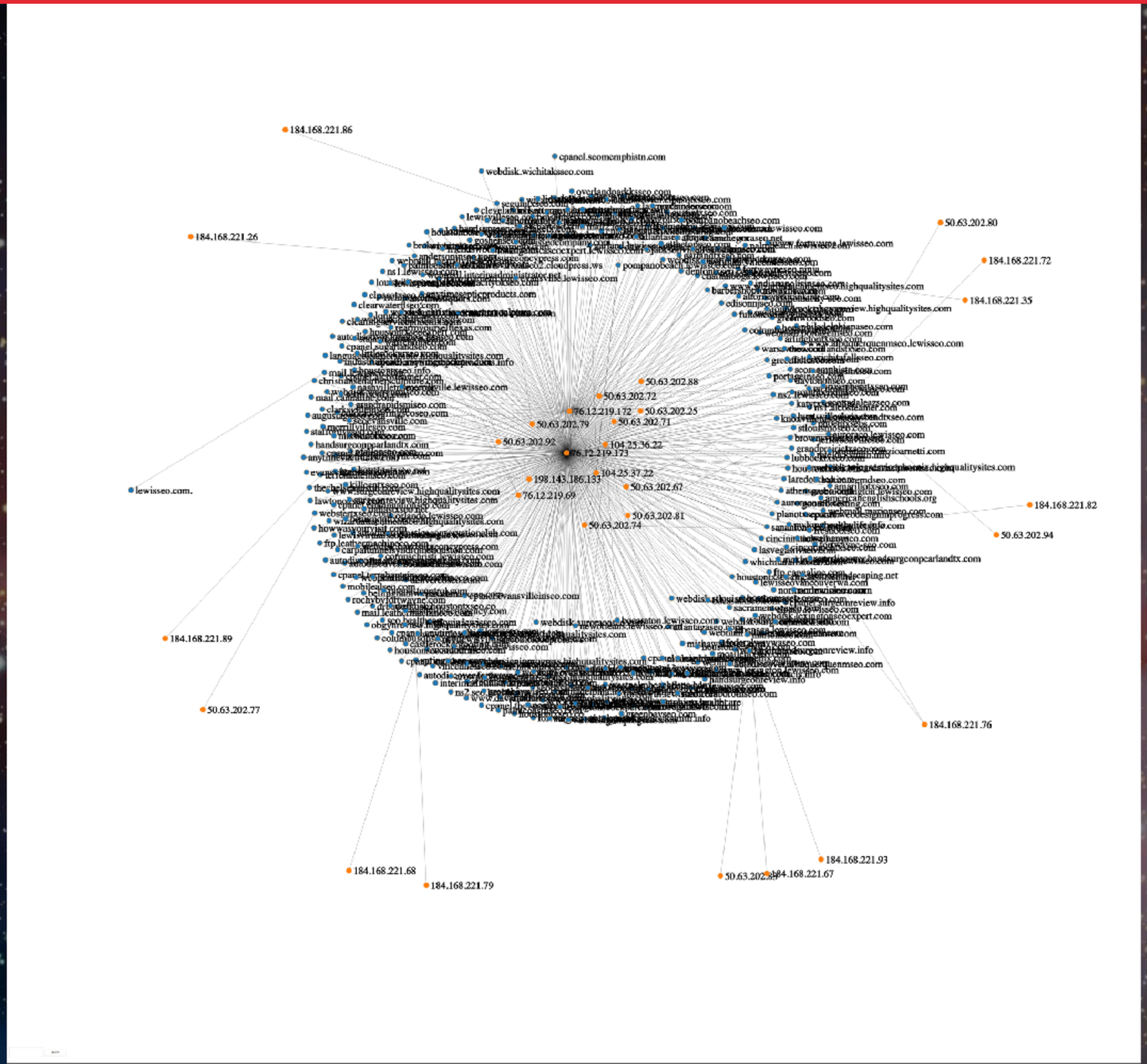

Node: 76.12.219.172
Degree: 1
IP: True


Node: 76.12.219.173
Degree: 2
IP: True

ENRICHING THOSE SMALL CONNECTIONS TO FIND ADDITIONAL RELATIONSHIPS



TURN LABELS ON TO ELABORATE THE RELATIONSHIPS

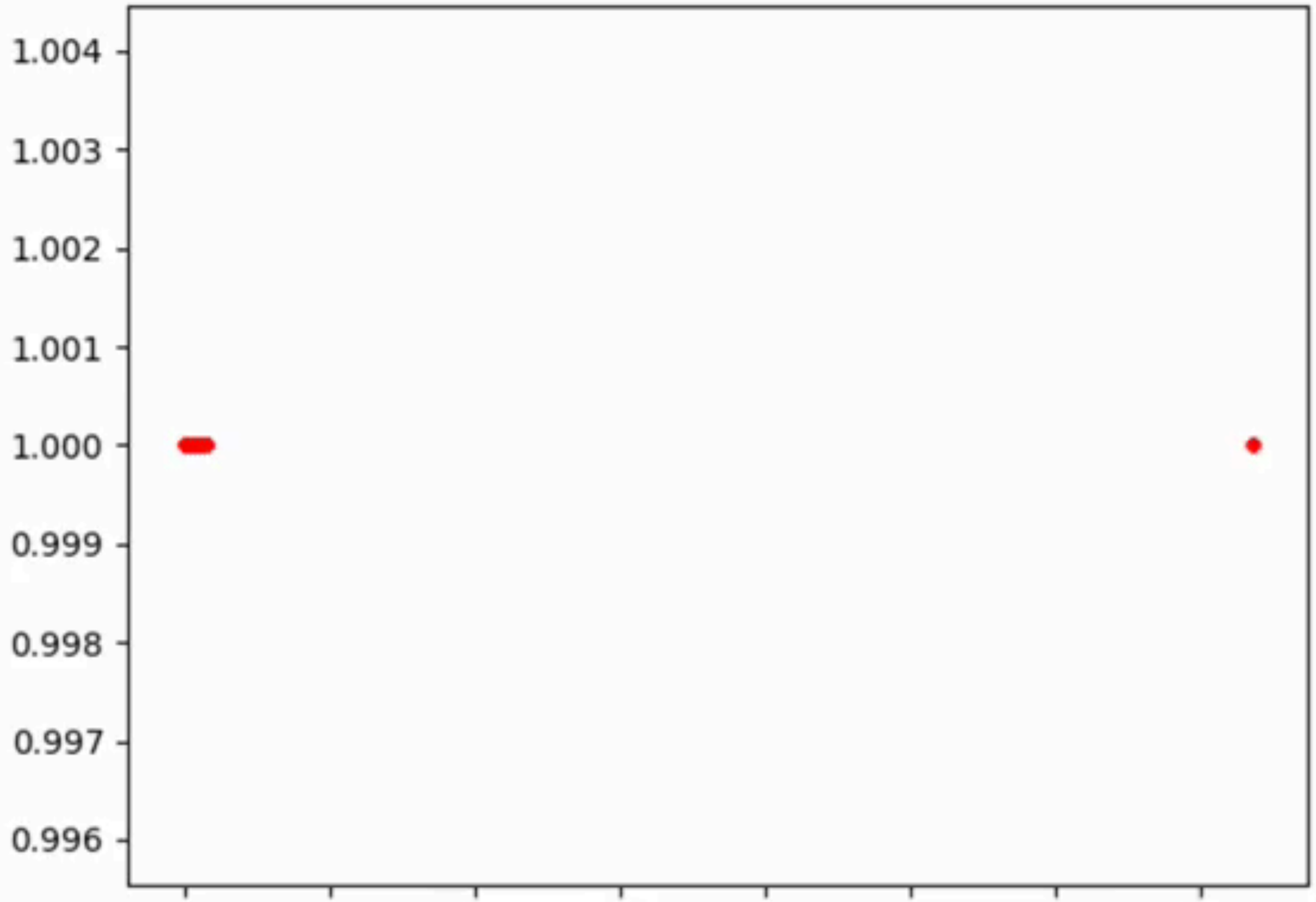


TIMELINES

VIEWING ALL THE TRICKBOT DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS

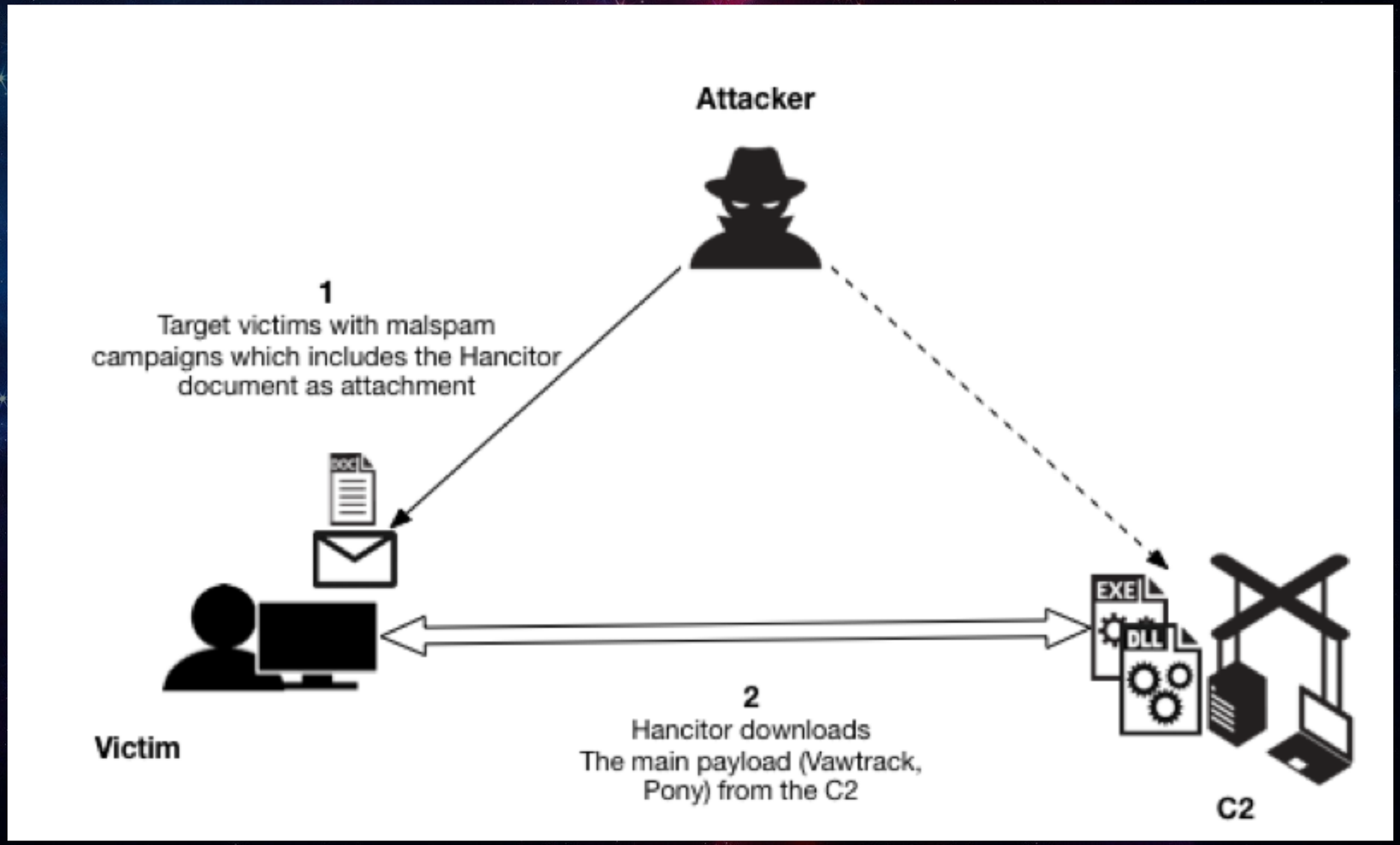
PATTERNS

2018-06-14-Emotet-infection-traffic-with-Trickbot.png Open with Preview

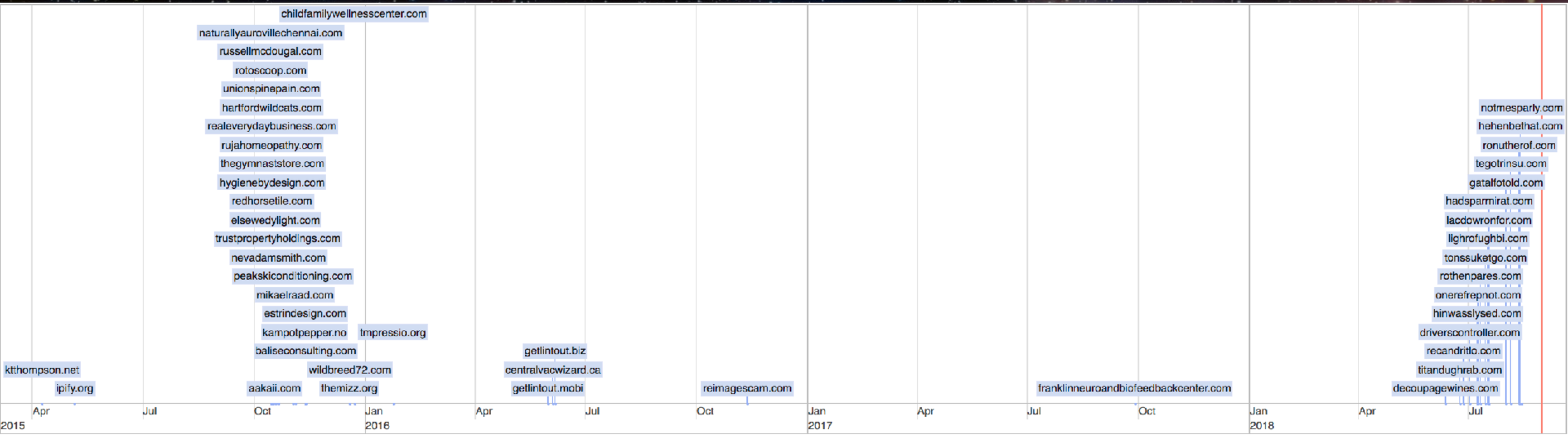


LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

HANCITOR

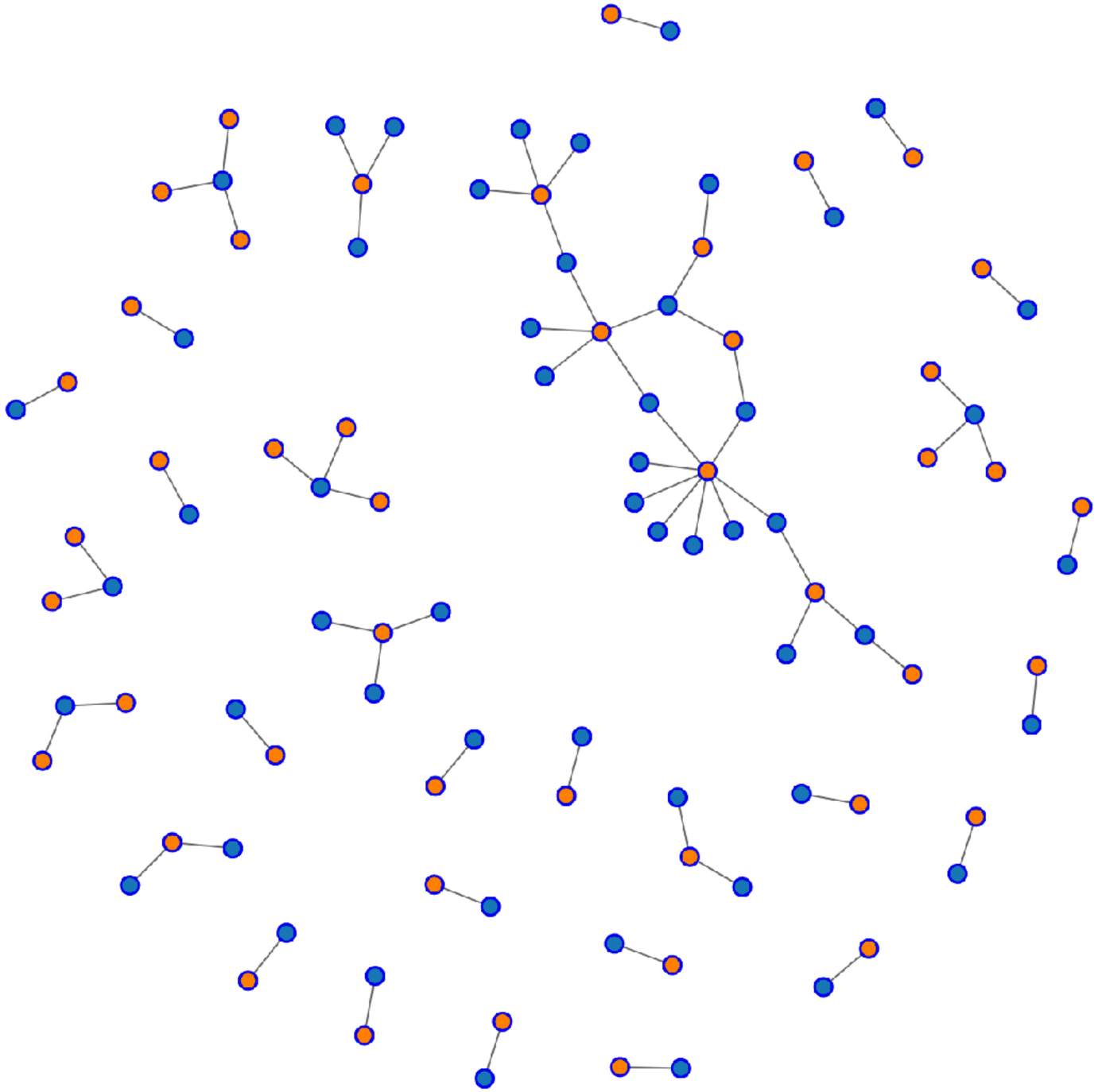

Attacker
1
Target victims with malspam campaigns which includes the Hancitor document as attachment
doc
EXE
DLL
Victim
2
Hancitor downloads
The main payload (Vawtrack, Pony) from the C2
C2

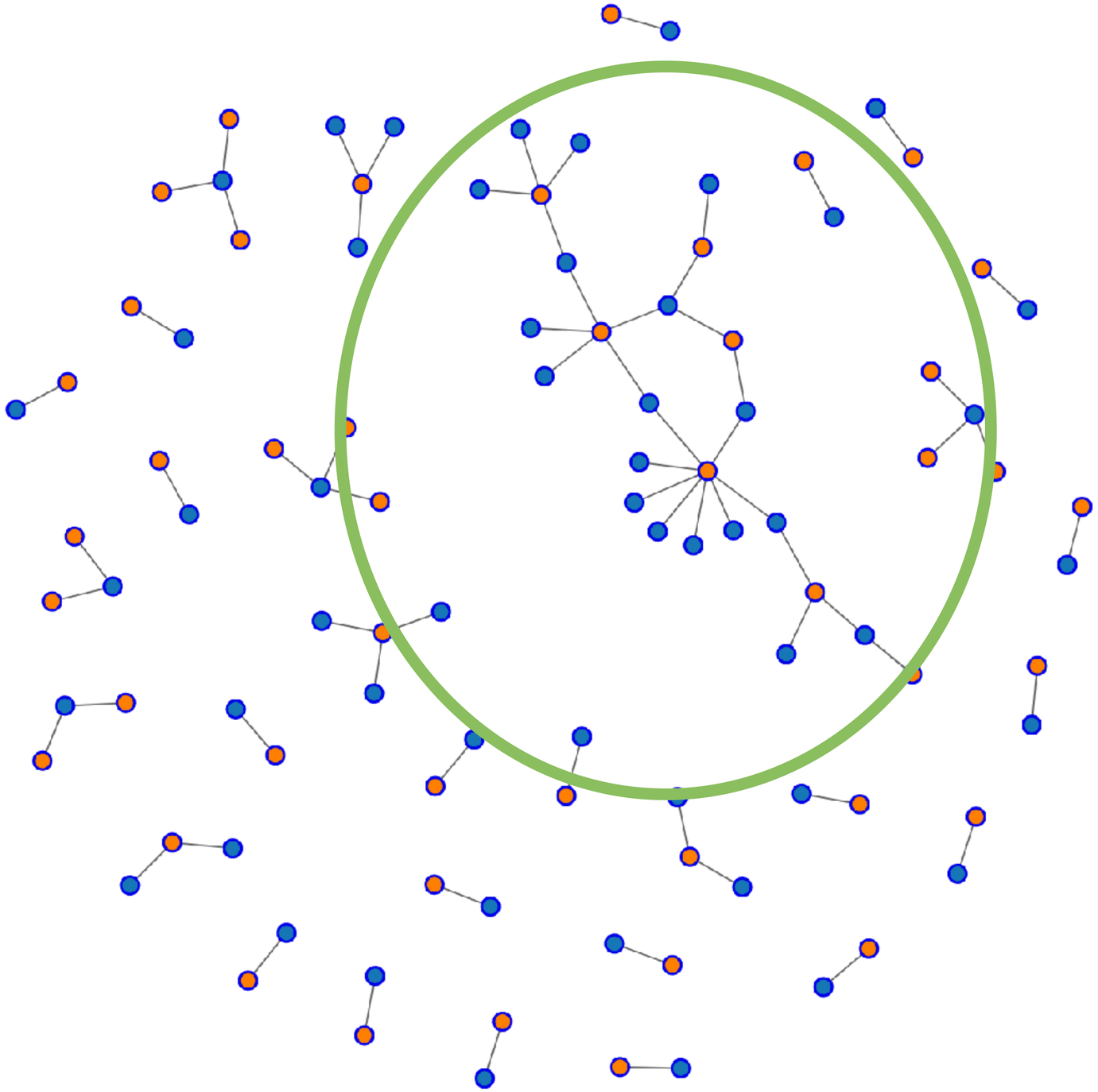
TIMELINES

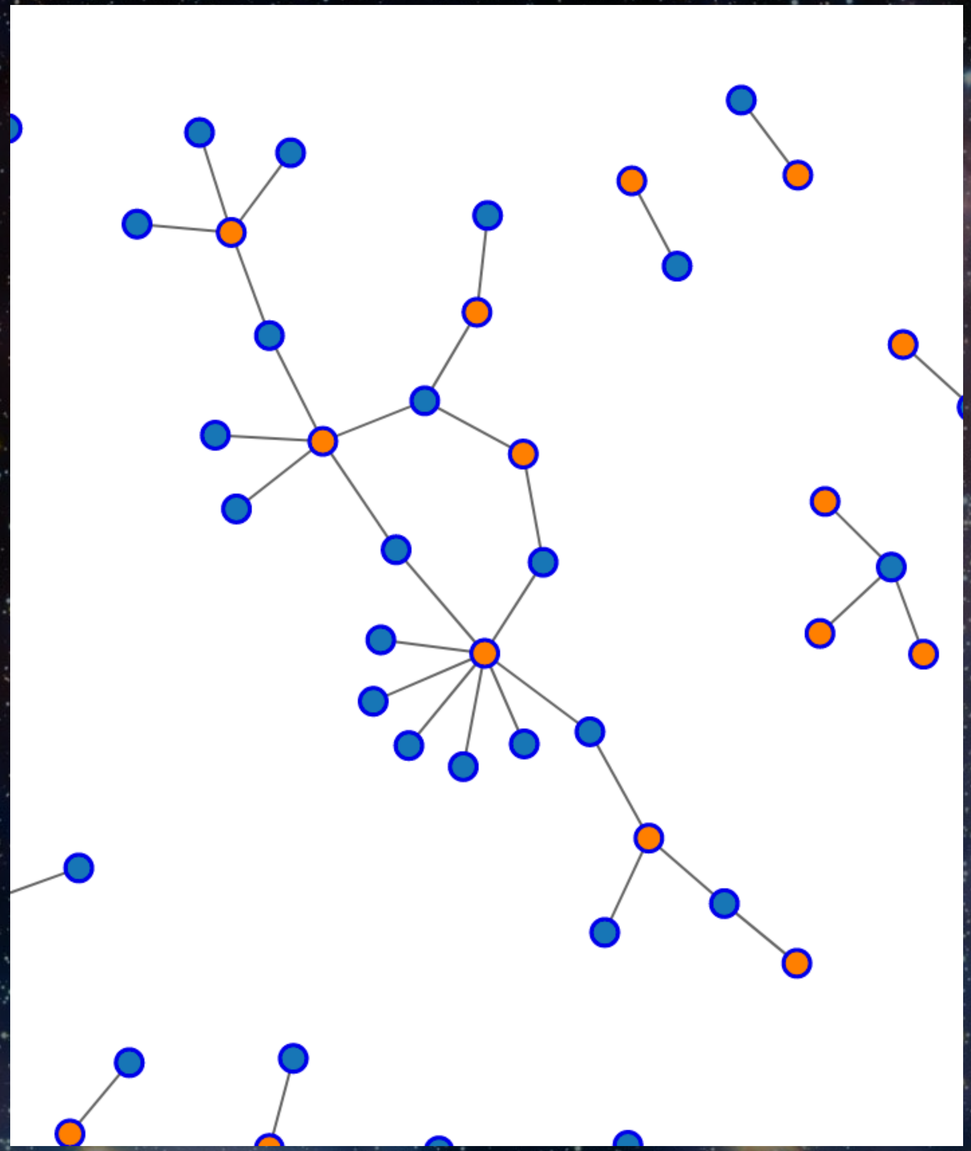


VIEWING ALL THE HANCITOR DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS

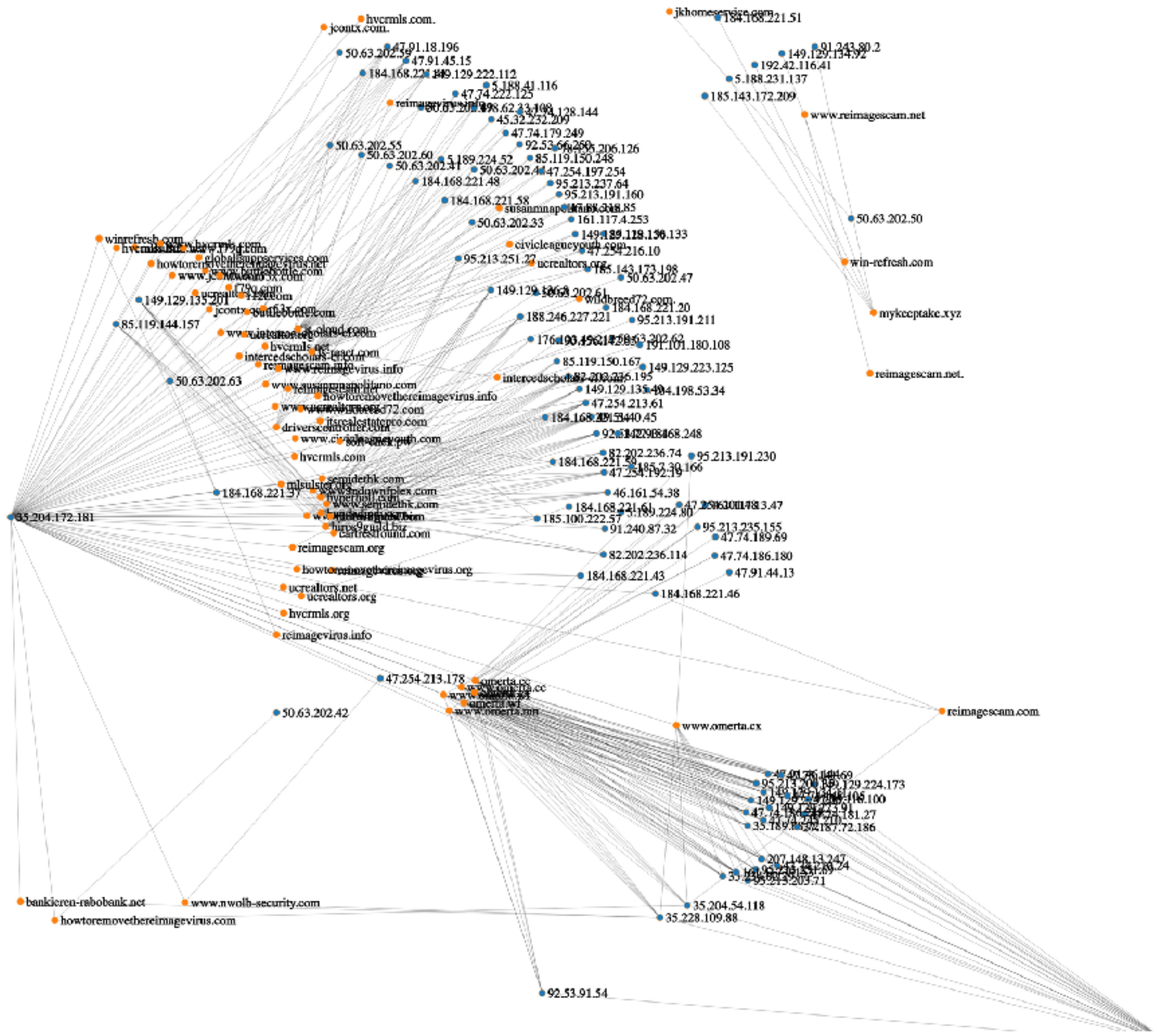
FORCE DIRECTED GRAPH



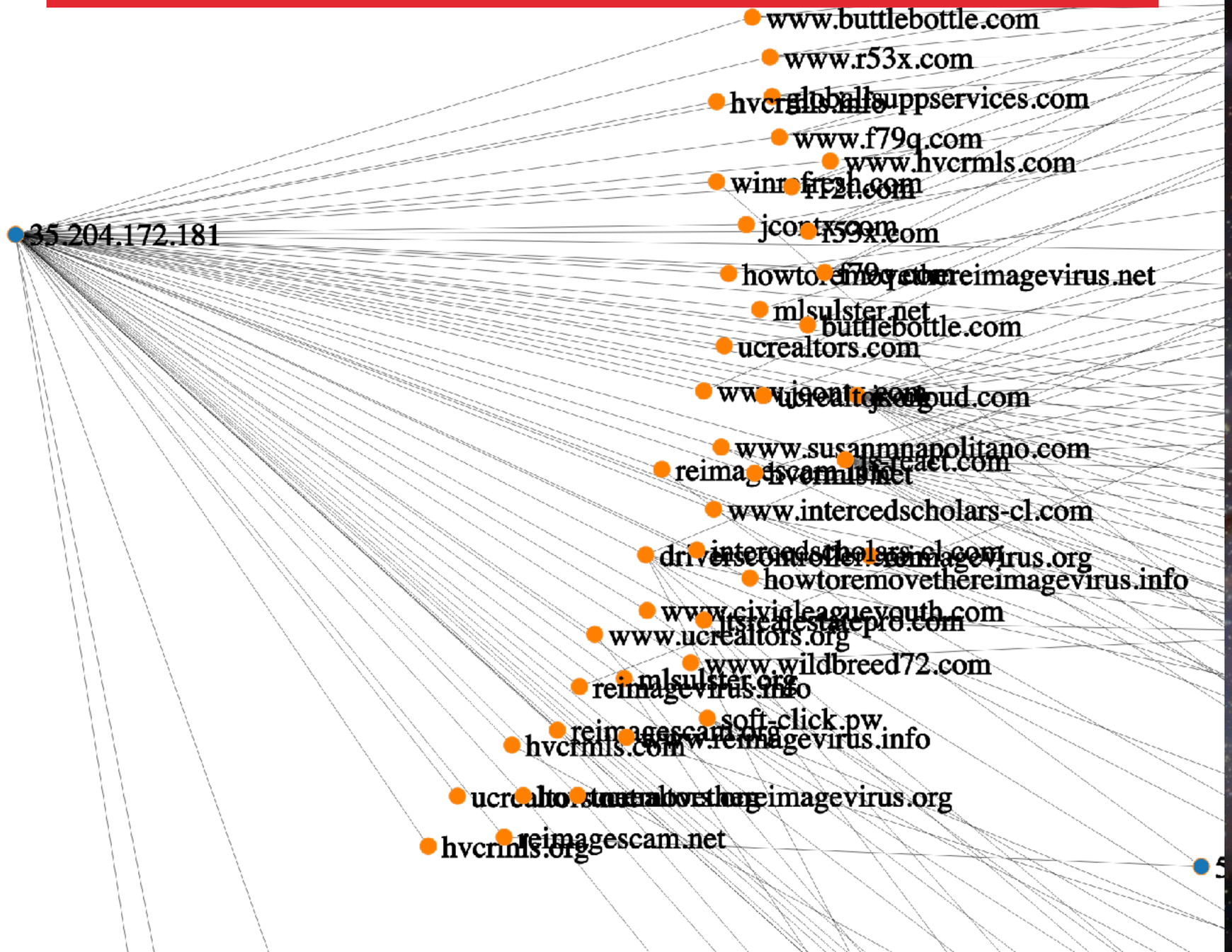




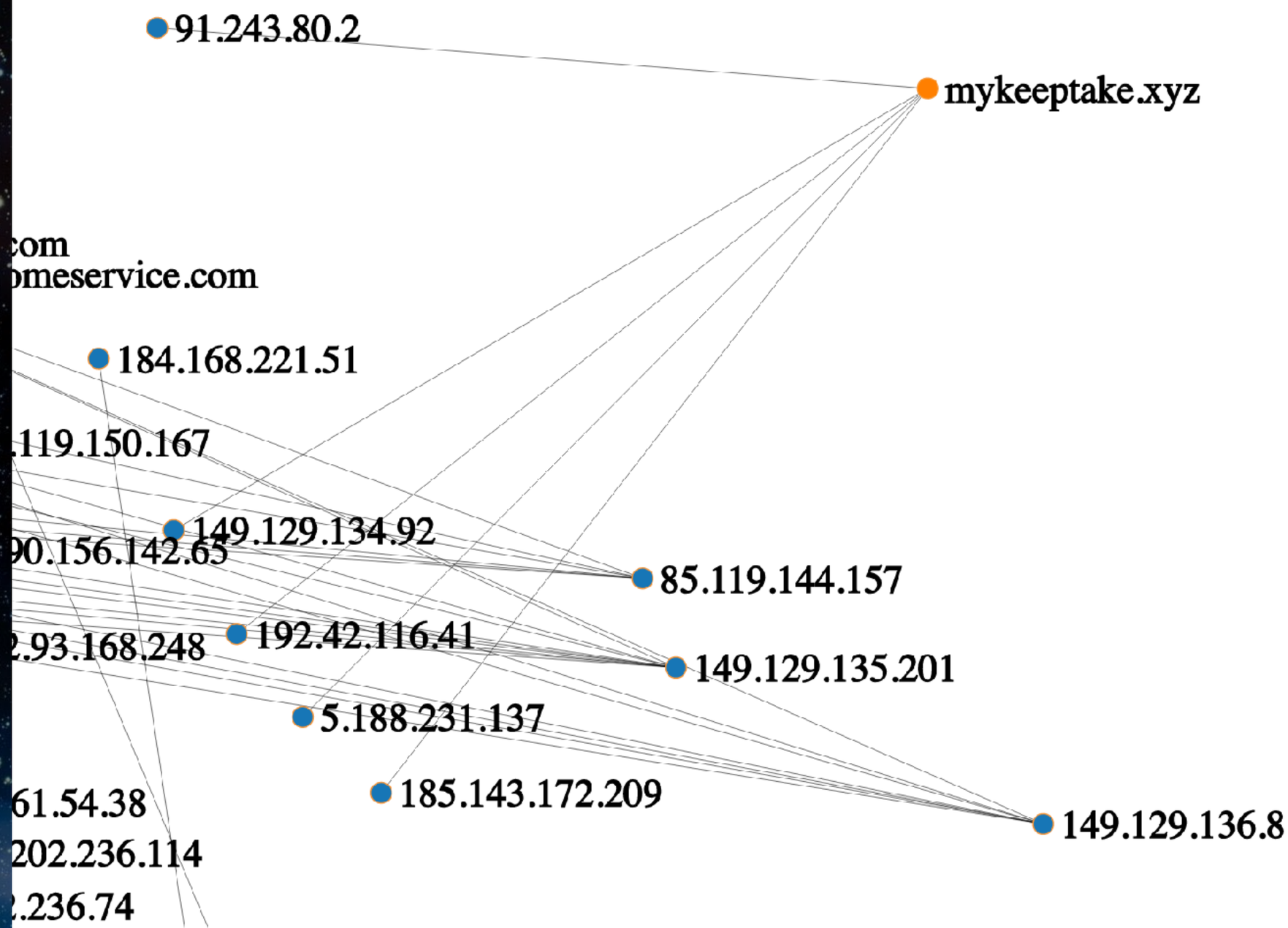
TURN LABELS ON TO ELABORATE THE RELATIONSHIPS



TURN LABELS ON TO ELABORATE THE RELATIONSHIPS

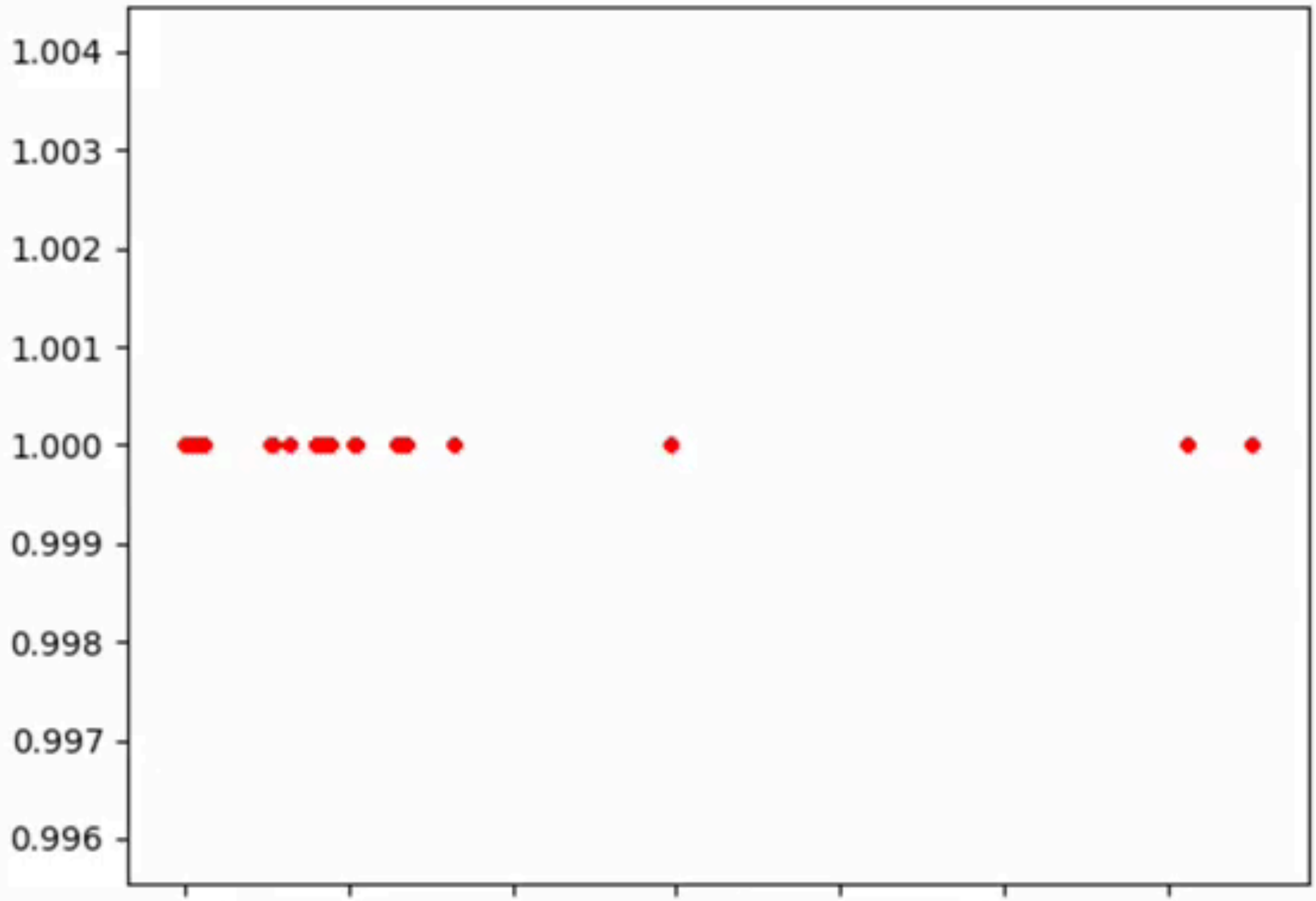


WE SEE MYKEEPTAKE.XYZ, FROM EMOTET IN HANCITOR TOO



PATTERNS

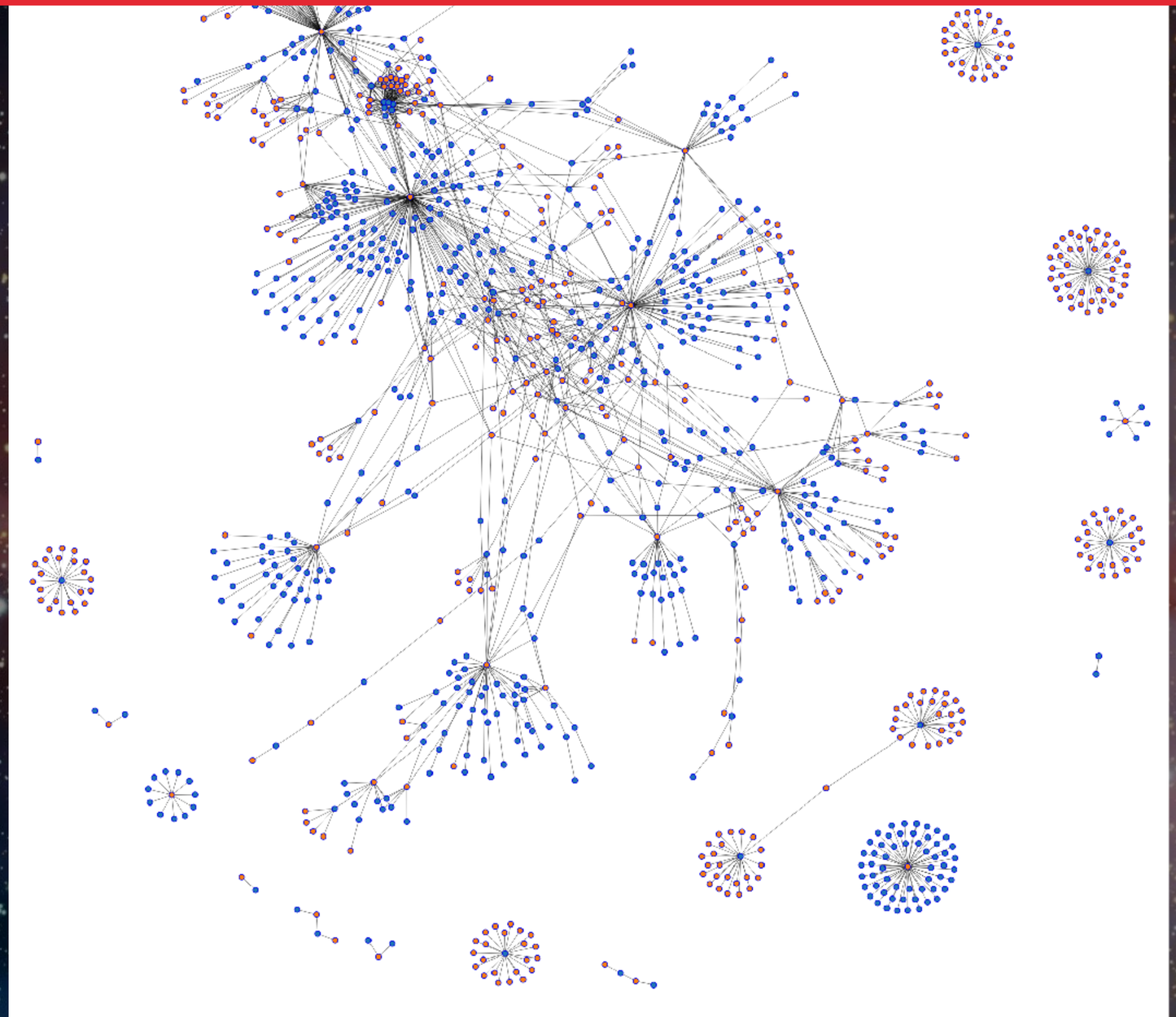
2018-06-28-Hancitor-malspam-infection-traffi.png Open with Preview



LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

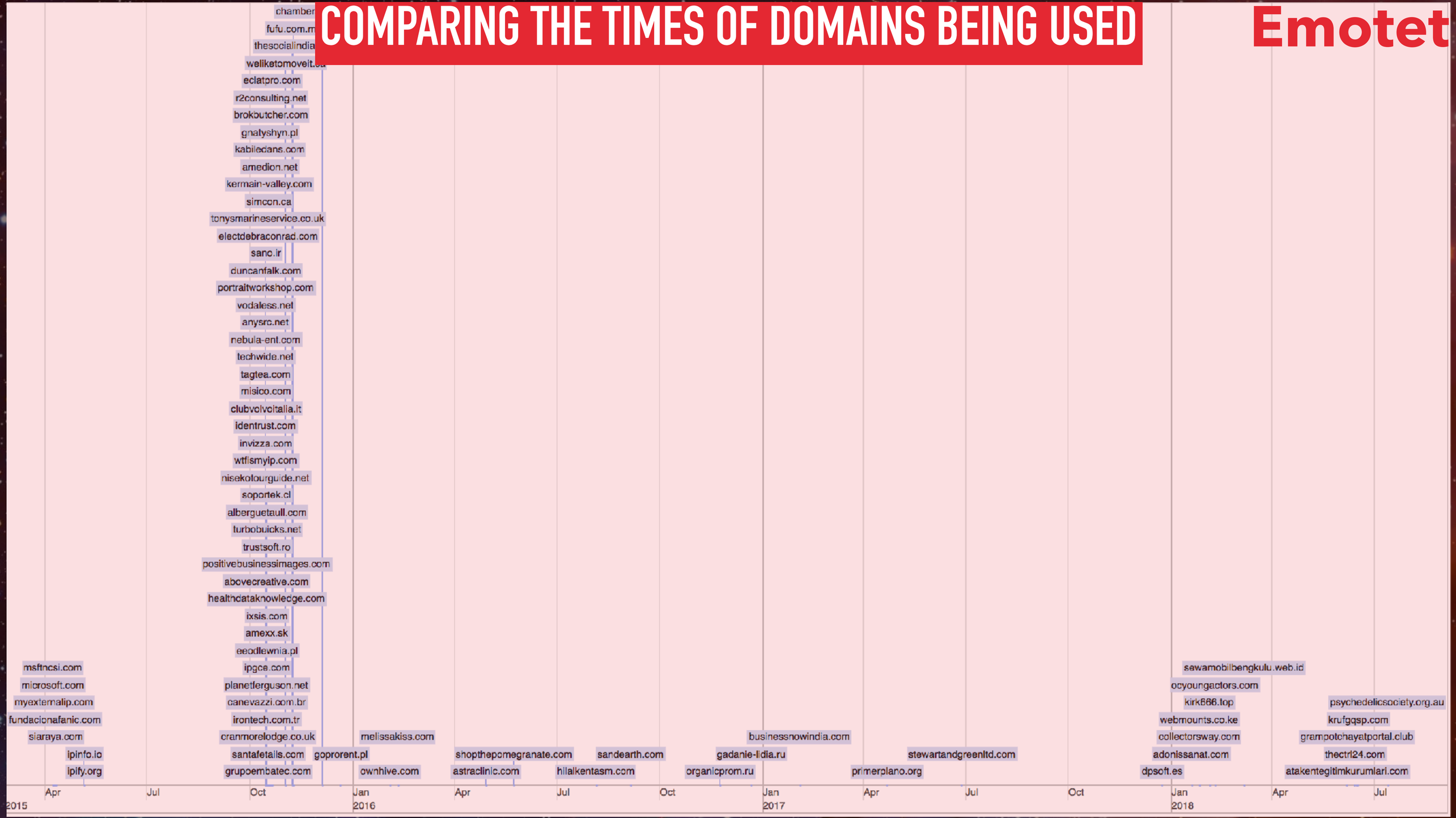
RELATIONSHIPS BETWEEN ATTACK INFRASTRUCTURE

VIEWING TRICKBOT, EMOTET, AND HANCITOR ALL TOGETHER TO FIND SHARED INFRASTRUCTURE

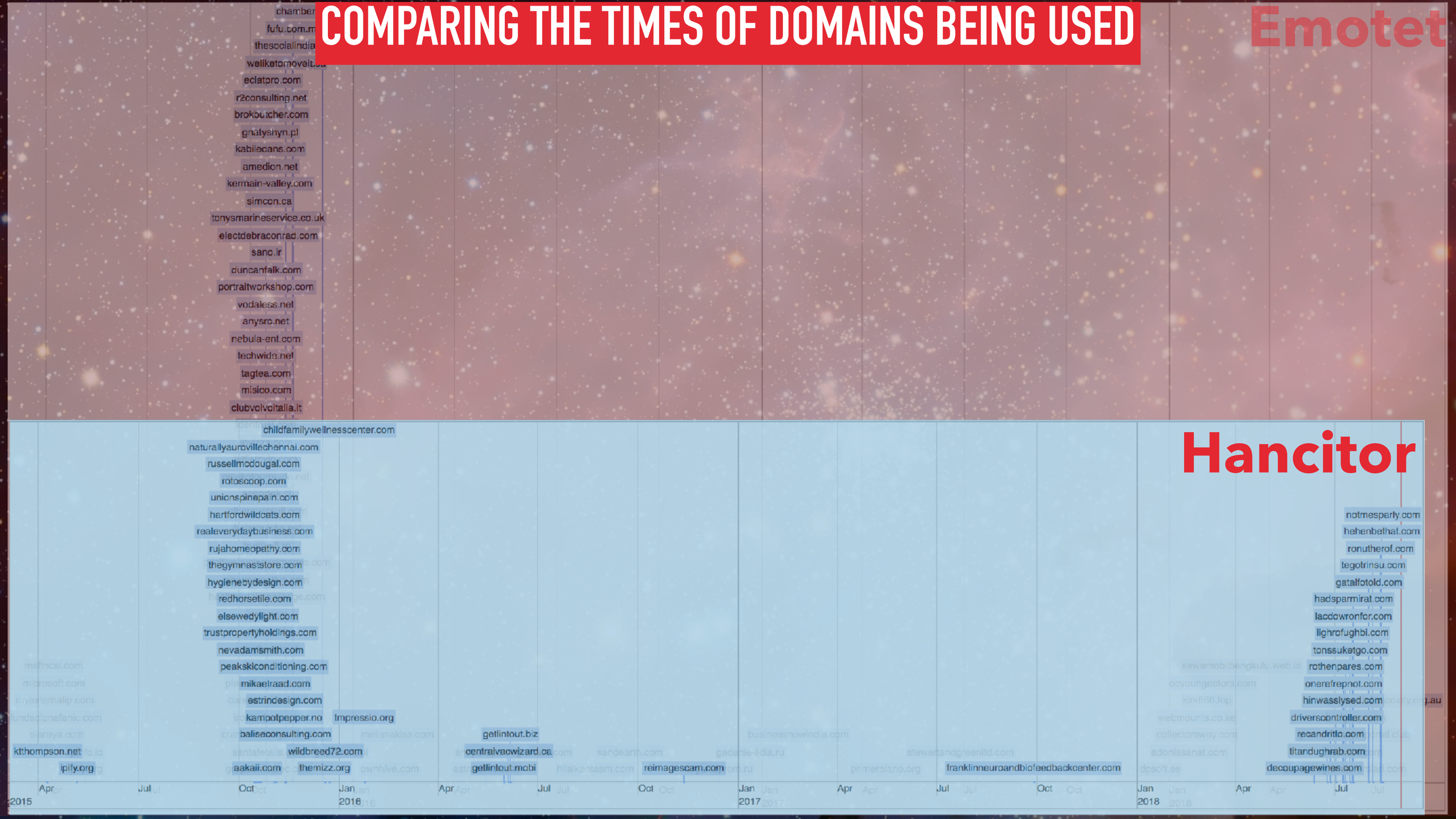


COMPARING THE TIMES OF DOMAINS BEING USED

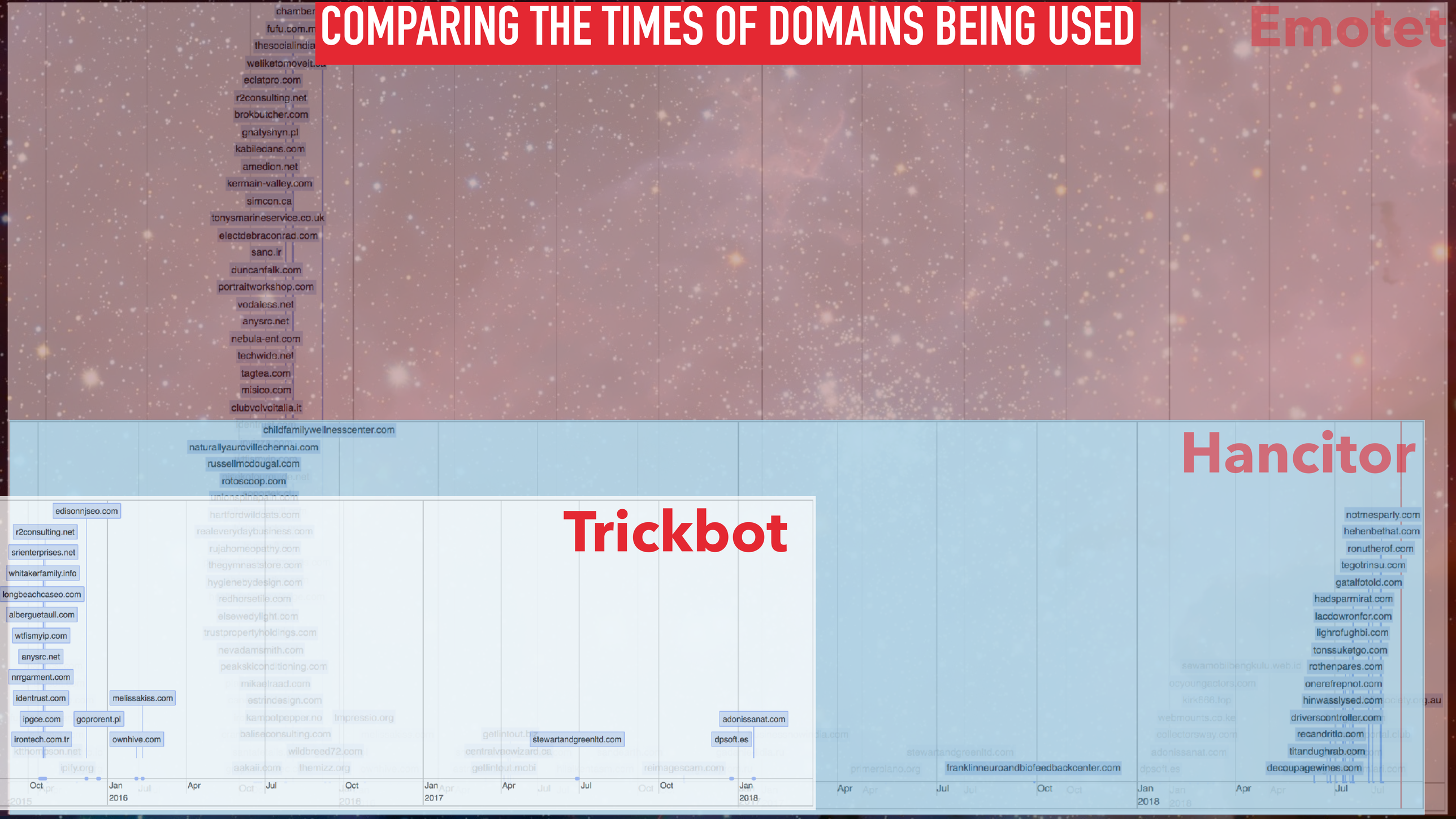
Emotet



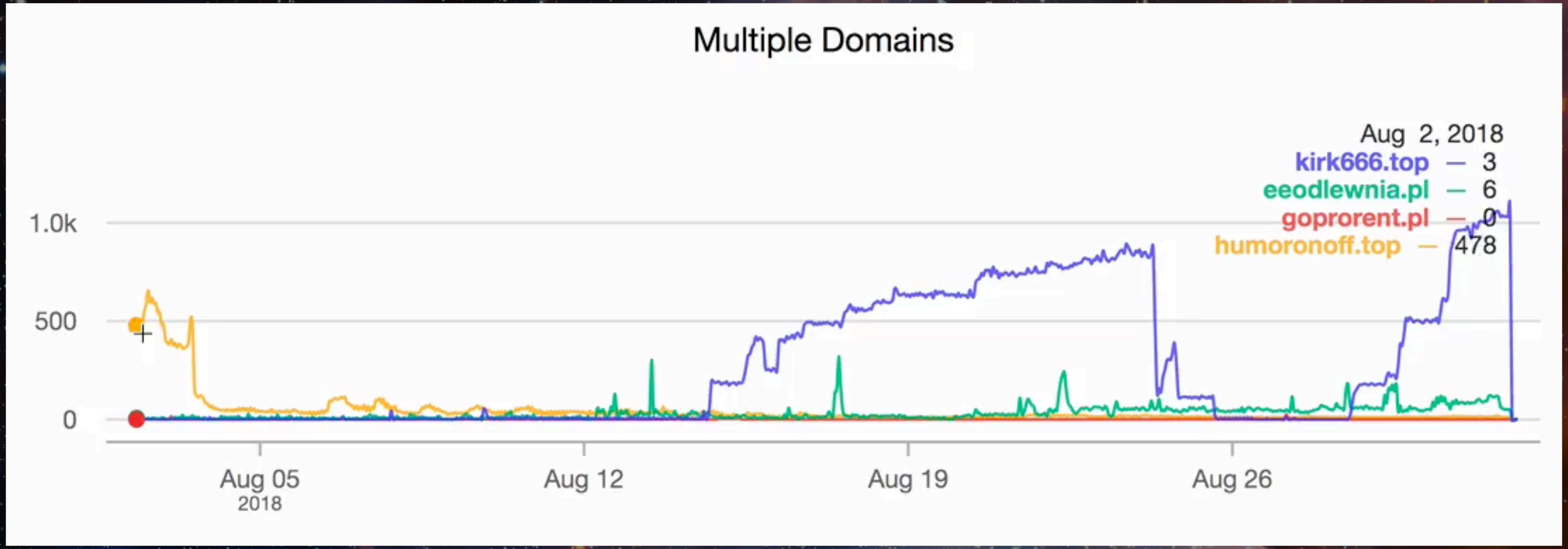
COMPARING THE TIMES OF DOMAINS BEING USED



COMPARING THE TIMES OF DOMAINS BEING USED



COMPARING THE QUERIES OF DOMAINS BEING USED



QUESTIONS?

CODE: https://pyosec.com

@AScarf0 @joshpyorre