



INTELLIGENT
DEFENCE

infosecurity®
EUROPE



Josh Pyorre, Security Researcher

BEHAVIORAL ANALYSIS USING DNS & NETWORK TRAFFIC



Here's how visitors behave on our website!

Video of User Analysis During Web Browsing



Video of Behavioral Analysis Anomaly Detection of a Crowd

Identification of pedestrians, events or observations which do not conform to an expected pattern or movement of other pedestrians in a crowd.



DETECTION METHODS

- IDS
- AntiVirus
- People



IDS

- Based on Signatures



IDS

```
#alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"ET  
WEB_SERVER PHP Generic Remote File Include Attempt (HTTP)";  
flow:to_server,established; content:".php"; nocase; http_uri;  
content:"=http|3a|/"; nocase; http_uri;  
pcr:"/\x2Ephp\x3F.{0,300}\x3Dhttp\x3A\x2F[^\x3F\x26]+\x3F/Ui";  
reference:url,doc.emergingthreats.net/2009151; classtype:web-application-  
attack; sid:2009151; rev:7;)
```



IDS

- Based on Signatures
- Requires Human Intervention
- Catches Known Threats
- Not Really Predictive



ANTIVIRUS

AVG PC TuneUp 2014

Keep your PC in tip-top condition - always!

- ✓ Reduce the load on your PC to practically zero
- ✓ Delete program remnants and unnecessary Windows files
- ✓ Use 1-Click Maintenance for all-round care of your PC
- ✓ Clean up traces of surfing activity and optimize your browser databases
- ✓ Increase battery life by up to 30%



Your trial period has expired!

Enter product key

Buy now



ANTIVIRUS

- Host-based
- Signatures for Known Threats



WHAT WE'RE WORKING WITH



Date	Time	Record Type	Internal IP Address	External IP Address	Action	Destination	Categories			
10/28/16	7:59:56	A	N/A	96.91.38.193	Allowed	ncod43.n-ab	Business Services			
10/28/16	7:59:28	A	N/A	96.91.38.193	Allowed	ej.crpasport.com				
10/28/16	7:58:59	A	N/A	108.212.122	Allowed	tools.google	Search Engines,Software/Technology			
10/28/16	7:58:28	A	N/A	96.91.38.193	Allowed	www.micros	Software/Technology,Business Services			
10/28/16	7:58:25	A	N/A	96.91.38.193	Allowed	www.google	Search Engines			
10/28/16	7:58:20	A	N/A	96.91.38.193	Allowed	ncod43.n-ab	Business Services			
10/28/16	7:56:14	A	N/A	96.91.38.193	Allowed	ncod43.n-ab	Business Services			
10/28/16	7:55:58	A	N/A	108.212.122	Allowed	teredo.ipv6	Software/Technology,Business Services			
10/28/16	7:55:37	A	N/A	96.91.38.193	Allowed	client.tear	Software/Technology,Business Services			
10/28/16	7:55:05	SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.default-first-site-name_sites.dc_msdc	econtrols.us			
10/28/16	7:55:05	SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.dc_msdc	econtrols.us			
10/28/16	7:54:24	A	N/A	96.91.38.193	Allowed	ej.crpasport.com				
10/28/16	7:53:56	A	N/A	96.91.38.193	Allowed	econtrols.us				
10/28/16	7:53:34	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:34	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:33	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:33	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:33	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:33	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:32	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:32	A	N/A	96.91.38.193	Allowed	upgrade.bitd	Software/Technology,Business Services			
10/28/16	7:53:18	A	N/A	96.91.38.193	Allowed	ncod43.n-ab	Business Services			
10/28/16	7:53:04	SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.dc_msdc	econtrols.us			
10/28/16	7:53:04	SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.default-first-site-name_sites.dc_msdc	econtrols.us			
10/28/16	7:52:46	SRV	N/A	96.91.38.193	Allowed	kerberos.tco.dc.msdc	exocontrols.com			



2016-10-31-pseudoDarkleech-MIGV-delivers-Cerber-ransomware.pcap

Apply a display filter ... <36/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.31.103	192.185.225.245	TCP	60	49191 → 80 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000000	192.185.225.245	10.10.31.103	TCP	60	80 → 49191 [SYN, ACK] Seq=0 Ack=1 Min=64240 Len=0 MSS=1460
3	0.000000	10.10.31.103	192.185.225.245	TCP	60	49191 → 80 [ACK] Seq=1 Ack=1 Min=64240 Len=0
4	0.000000	10.10.31.103	192.185.225.245	HTTP	384	GET / HTTP/1.1
5	0.000000	192.185.225.245	10.10.31.103	TCP	60	80 → 49191 [ACK] Seq=1 Ack=251 Min=64240 Len=0
6	1.000000	192.185.225.245	10.10.31.103	TCP	568	[TCP segment of a reassembled PDU]
7	1.000000	10.10.31.103	192.185.225.245	TCP	60	49191 → 80 [ACK] Seq=151 Ack=515 Min=63736 Len=0

▶ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: HewlettP_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93:f1 (28:e5:12:a6:93:f1)
 ▶ Internet Protocol Version 4, Src: 10.10.31.103 (10.10.31.103), Dst: 192.185.225.245 (192.185.225.245)
 ▶ Transmission Control Protocol, Src Port: 49191 (49191), Dst Port: 80 (80), Seq: 0, Len: 0

```

0000  20 e5 2a b6 93 f1 00 00 02 1c 47 ae 00 00 45 00  .*. ....E.
0010  00 34 02 b3 40 00 00 06 2b f1 8a 0a 1f 67 c0 b0  .4..0...+...g..
0020  e1 15 c8 27 00 50 ed 25 98 8c 00 00 00 00 02    ...P.% .....
0030  20 00 44 c6 00 00 02 04 05 b4 01 03 03 00 01 01  .0.....
0040  04 02
  
```

PCAP'S



Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security**
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 181,534 (1) New events available

Keywords	Date and Time	Task Category
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	Other Object Access Events
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	SAM
Audit Success	11/4/2014 6:31:50 AM	Process Termination
Audit Success	11/4/2014 6:31:50 AM	Process Creation
Audit Success	11/4/2014 6:31:47 AM	Process Termination
Audit Success	11/4/2014 6:31:47 AM	Process Creation

AD logs

Actions

Security

- Op...
- Cr...
- Im...
- Cle...
- Fit...
- Pro...
- Fin...
- Se...
- Att...
- View
- Re...
- Help



"cs_host", "cs_uri_path", "cs_uri_quer
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED
"na10.salesforce.com", "/", , PROXIED



1472145600 pagead.l.doubleclick.net. A 300 216.58.212.130 216.239.38.10 doubleclick.net.

1472145600 tctirefactory.com. MX 86400 aspmx2.googlemail.com. 65.61.188.4 tctirefactory.com.

1472145600 tctirefactory.com. MX 86400 alt1.aspmx.l.google.com. 65.61.188.4 tctirefactory.com.

1472145600 tctirefactory.com. MX 86400 aspmx3.googlemail.com. 65.61.188.4 tctirefactory.com.

1472145600 tctirefactory.com. MX 86400 alt2.aspmx.l.google.com. 65.61.188.4 tctirefactory.com.

1472145600 tctirefactory.com. MX 86400 aspmx.l.google.com. 65.61.188.4 tctirefactory.com.

1472145600 xp.itunes-apple.com.akadns.net. CNAME 300 mt-ingestion-service-mr22.itunes.apple.com. 184.85.248.128 akadns.net.

1472145600 s.youtube.com. CNAME 3600 videotat.l.google.com. 216.239.36.10 youtube.com.

1472145600 mt-ingestion-service-mr22.itunes-apple.com.akadns.net. A 300 17.110.234.28 2.22.230.130 akadns.net.

1472145600 mt-ingestion-service-mr22.itunes-apple.com.akadns.net. A 300 17.110.232.46 2.22.230.130 akadns.net.

1472145600 mt-ingestion-service-mr22.itunes-apple.com.akadns.net. A 300 17.110.234.27 2.22.230.130 akadns.net.

1472145600 mt-ingestion-service-mr22.itunes-apple.com.akadns.net. A 300 17.110.232.45 2.22.230.130 akadns.net.

1472145600 ns-1114.awsdns-11.org. A 172800 205.251.196.90 205.251.196.14 awsdns-11.org.

1472145600 geo.vortex.data.microsoft.com.akadns.net. CNAME 300 geo.vortex.data.microsoft.com.akadns.net. 84.53.139.129 akadns.net.

1472145600 www.googleadservices.com. CNAME 300 pagead.l.doubleclick.net. 216.239.32.10 googleadservices.com.

1472145600 sna-kantata.ru. A 3600 141.8.195.73 78.140.198.146 sna-kantata.ru.

1472145600 mx1.alt-comision.ru. A 600 178.208.83.91 91.134.50.205 alt-comision.ru.

1472145600 p42-ckdevice-current.edge.icloud.apple-dns.net. A 30 17.248.150.106 205.251.195.252 icloud.apple-dns.net.

1472145600 lb2-543841419.us-east-1.elb.amazonaws.com. A 60 52.202.211.163 205.251.196.95 us-east-1.elb.amazonaws.com.

1472145600 lb2-543841419.us-east-1.elb.amazonaws.com. A 60 52.204.135.45 205.251.196.95 us-east-1.elb.amazonaws.com.

1472145600 mail.airband.net. A 300 67.225.220.14 207.34.46.25 airband.net.

1472145600 origin.guzzoni-apple.com.akadns.net. CNAME 300 mu21p02sa.guzzoni-apple.com.akadns.net. 2.22.230.130 akadns.net.



File Home Insert Page Layout Formulas Data Review View

Paste Calibri (Body) 12 A A = = = Wrap Text General Conditional Formatting Format as Table Cell Styles Insert Delete Format

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Date	Time	Record Type	Internal IP Address	External IP Address	Action	Destination	Categories							
2	10/28/16	7:59:56 A	N/A	96.91.38.193	Allowed	ncod43.n-able.com	Business Services								
3	10/28/16	7:59:28 A	N/A	96.91.38.193	Allowed	ej.crpasport.com									
4	10/28/16	7:58:59 A	N/A	108.212.122	Allowed	tools.google.com	Search Engines,Software/Technology								
5	10/28/16	7:59:28 A	N/A	96.91.38.193	Allowed	www.microsoft.com	Software/Technology,Business Services								
6	10/28/16	7:59:25 A	N/A	96.91.38.193	Allowed	www.google.com	Search Engines								
7	10/28/16	7:59:20 A	N/A	96.91.38.193	Allowed	ncod43.n-able.com	Business Services								
8	10/28/16	7:59:14 A	N/A	96.91.38.193	Allowed	ncod43.n-able.com	Business Services								
9	10/28/16	7:59:58 A	N/A	108.212.122	Allowed	teredo.ipv6.microsoft.com	Software/Technology,Business Services								
10	10/28/16	7:55:37 A	N/A	96.91.38.193	Allowed	client.teamviewer.com	Software/Technology,Business Services								
11	10/28/16	7:55:05 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.default-first-site-name_sites.dc_msdc.econtrols.us									
12	10/28/16	7:55:05 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.dc_msdc.econtrols.us									
13	10/28/16	7:54:24 A	N/A	96.91.38.193	Allowed	ej.crpasport.com									
14	10/28/16	7:53:56 A	N/A	96.91.38.193	Allowed	econtrols.us									
15	10/28/16	7:53:34 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
16	10/28/16	7:53:34 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
17	10/28/16	7:53:33 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
18	10/28/16	7:53:33 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
19	10/28/16	7:53:33 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
20	10/28/16	7:53:33 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
21	10/28/16	7:53:32 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
22	10/28/16	7:53:32 A	N/A	96.91.38.193	Allowed	upgrade.bitdefender.com	Software/Technology,Business Services								
23	10/28/16	7:53:18 A	N/A	96.91.38.193	Allowed	ncod43.n-able.com	Business Services								
24	10/28/16	7:53:04 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.dc_msdc.econtrols.us									
25	10/28/16	7:53:04 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.default-first-site-name_sites.dc_msdc.econtrols.us									
26	10/28/16	7:52:46 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.dc_msdc.expcontrols.com									
27	10/28/16	7:52:46 SRV	N/A	96.91.38.193	Allowed	_kerberos_tcp.default-first-site-name_sites.dc_msdc.expcontrols.com									
28	10/28/16	7:52:46 A	N/A	96.91.38.193	Allowed	mex09.emailsrvr.com	Webmail								
29	10/28/16	7:52:34 A	N/A	96.91.38.193	Allowed	ncod43.n-able.com	Business Services								
30	10/28/16	7:50:00 A	N/A	96.91.38.193	Allowed	secure.autodiscover.emailsrvr.com	Webmail								
31	10/28/16	7:49:59 A	N/A	96.91.38.193	Allowed	autodiscover.emailsrvr.com	Webmail								
32	10/28/16	7:49:58 A	N/A	96.91.38.193	Allowed	expcontrols.com									
33	10/28/16	7:49:50 A	N/A	108.212.122	Allowed	www.microsoft.com	Software/Technology,Business Services								
34	10/28/16	7:49:20 A	N/A	96.91.38.193	Allowed	ej.crpasport.com									
35	10/28/16	7:49:05 A	N/A	108.212.122	Allowed	teredo.ipv6.microsoft.com	Software/Technology,Business Services								

Video of log analysis in Excel

FINDING NORMAL

- What is Normal?
- How Do You Find It?



comserver.global.mspa.n-able.com
gv.symcd.com
adadvisor.net
adadvisor.net
adadvisor.net
agkn.com
d.agkn.com
d.agkn.com
su.addthis.com
su.addthis.com
su.addthis.com

Video of a Suspicious domain in logs

[illegible]

seg-server-lb.global.prod1.sharethis.net

t.sharethis.com

sb.scorecardresearch.com

seq.sharethis.com

1.sharethis.com

analytics.localytics.com

wfbs-svc-nabu-aal.trendmicro.com

shared.iad.appboy.com

wfbssvc51.icrc.trendmicro.com

staticxx.facebook.com

script.crazyegg.com

script.crazyegg.com

2016-09-22 22:55:05.283770 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.49062: 4644 2/0/0 CNAME ssl-google-analytics.l.google.com., A 216.58.194.168 (82)
2016-09-22 22:55:08.739970 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.51339: 32438 4/0/0 CNAME cdn.turner.com.edgekey.net., CNAME e2546.dsce4.akamaiedge.net., AAAA 2001:418:142b:280::9f2, AAAA 2001:418:142b:299::9f2 (167)
2016-09-22 22:55:08.923499 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.21617: 26983 3/0/0 CNAME cdn.turner.com.edgekey.net., CNAME e2546.dsce4.akamaiedge.net., A 23.34.169.228 (127)
2016-09-22 22:55:30.036644 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.33385: 19281 3/0/0 CNAME white.ish.instagram.com., CNAME instagram.c10r.facebook.com., AAAA 2a03:2880:f213:c4:face:b00c:0:43fe (127)
2016-09-22 22:55:30.073406 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.16977: 43171 3/0/0 CNAME white.ish.instagram.com., CNAME instagram.c10r.facebook.com., A 31.13.77.52 (115)
2016-09-22 22:55:40.111082 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.52058: 16191 1/0/0 A 216.58.217.196 (48)
2016-09-22 22:55:40.115764 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.52058: 45111 1/0/0 AAAA 2607:f8b0:4005:807::2004 (60)
2016-09-22 22:56:34.737197 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.24735: 26544 13/0/0 CNAME lb.geo.office365.com., CNAME outlook.office365.com.g.office365.com., CNAME outlook-namwest.office365.com., AAAA 2a01:111:f400:7020::2, AAAA 2a01:111:f400:2d74::2, AAAA 2a01:111:f400:4821::2, AAAA 2a01:111:f400:505a::2, AAAA 2a01:111:f400:2c5e::2, AAAA 2a01:111:f400:142a::2, AAAA 2a01:111:f400:4814::2, AAAA 2a01:111:f400:f3d3::2, AAAA 2603:1036:404:69::2, AAAA 2a01:111:f400:528b::2 (408)
2016-09-22 22:56:34.759200 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.10948: 25934 12/0/0 CNAME lb.geo.office365.com., CNAME outlook.office365.com.g.office365.com., CNAME outlook-namwest2.office365.com., A 132.245.46.130, A 132.245.47.66, A 132.245.56.146, A 40.97.142.234, A 132.245.71.2, A 132.245.73.194, A 132.245.75.114, A 132.245.92.242, A 132.245.82.50 (273)
2016-09-22 22:56:34.844883 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.40131: 53540 0/0/0 (38)
2016-09-22 22:56:34.864445 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.11446: 2946 1/0/0 A 72.163.8.7 (54)
2016-09-22 22:56:42.821722 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.41588: 63511 1/0/0 A 216.58.217.196 (48)
2016-09-22 22:56:42.826382 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.41588: 18168 1/0/0 AAAA 2607:f8b0:4005:807::2004 (60)
2016-09-22 22:57:36.931936 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.12528: 25205 1/1/0 CNAME api.v.dropbox.com., (137)
2016-09-22 22:57:36.950147 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.20426: 21516 3/0/0 CNAME api.v.dropbox.com., A 108.160.172.237, A 108.160.172.205 (85)
2016-09-22 22:57:45.683778 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.55995: 32643 1/0/0 A 216.58.195.228 (48)
2016-09-22 22:57:45.688176 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.55995: 48654 1/0/0 AAAA 2607:f8b0:4005:807::2004 (60)
2016-09-22 22:58:11.184444 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.55039: 25039 2/0/0 CNAME googlehosted.l.googleusercontent.com., A 216.58.195.65 (48)
2016-09-22 22:58:11.230111 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.55039: 25039 2/0/0 CNAME googlehosted.l.googleusercontent.com., A 216.58.195.65 (48)
2016-09-22 22:58:11.396222 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.32744: 12744 1/0/0 A 216.58.195.228 (48)
2016-09-22 22:58:11.377777 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.32744: 12744 1/0/0 AAAA 2607:f8b0:4005:807::2004 (60)
2016-09-22 22:59:51.054016 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.60760: 32649 1/0/0 A 216.58.195.228 (48)
2016-09-22 22:59:51.058684 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.60760: 24886 1/0/0 AAAA 2607:f8b0:4005:808::2004 (60)
2016-09-22 23:00:12.743037 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.39986: 62413 2/0/0 CNAME googlehosted.l.googleusercontent.com., A 216.58.194.193 (88)
2016-09-22 23:00:12.765773 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.39986: 48679 2/0/0 CNAME googlehosted.l.googleusercontent.com., AAAA 2607:f8b0:4005:808::2001 (100)
2016-09-22 23:00:26.007846 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.48195: 31653 1/1/0 CNAME ec2-54-241-32-2.us-west-1.compute.amazonaws.com., (176)
2016-09-22 23:00:26.029479 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.31902: 41839 2/0/0 CNAME ec2-54-241-32-5.us-west-1.compute.amazonaws.com., A 54.241.32.5 (111)
2016-09-22 23:00:26.991719 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.36577: 33224 2/1/0 CNAME guardian.map.fastly.net., CNAME prod.guardian.map.fastlylb.net., (193)
2016-09-22 23:00:27.012840 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.4991: 64371 3/0/0 CNAME guardian.map.fastly.net., CNAME prod.guardian.map.fastlylb.net., A 151.101.41.111 (135)
2016-09-22 23:00:27.088700 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.48134: 9145 2/1/0 CNAME mobile-apps.guardianapis.com.global.prod.fastly.net., CNAME prod.a.ssl.global.fastlylb.net., (226)
2016-09-22 23:00:27.109685 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.33348: 43133 3/0/0 CNAME mobile-apps.guardianapis.com.global.prod.fastly.net., CNAME prod.a.ssl.global.fastlylb.net., A 151.101.41.104 (168)
2016-09-22 23:00:27.259973 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.58047: 4816 4/1/0 CNAME cdn-traffic-director.krxd.net., CNAME cdn-fastly.krxd.net., CNAME cdn-fastly.krxd.net.c.global-ssl.fastly.net., CNAME prod.c.ssl.global.fastlylb.net., (259)
2016-09-22 23:00:27.285813 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.57931: 41937 5/0/0 CNAME cdn-traffic-director.krxd.net., CNAME cdn-fastly.krxd.net., CNAME cdn-fastly.krxd.net.c.global-ssl.fastly.net., CNAME prod.c.ssl.global.fastlylb.net., A 151.101.40.175 (201)
2016-09-22 23:00:27.701533 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.15364: 52766 1/1/0 CNAME theguardian.com.ssl.d1.sc.omtrdc.net., (166)
2016-09-22 23:00:27.729268 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.15359: 21454 2/0/0 CNAME theguardian.com.ssl.d1.sc.omtrdc.net., A 66.235.136.195 (111)
2016-09-22 23:00:42.486728 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.39022: 64832 1/0/0 AAAA 2607:f8b0:4005:807::200e (65)
2016-09-22 23:00:42.526826 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.64395: 62907 1/0/0 A 216.58.195.78 (53)
2016-09-22 23:00:53.805347 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.33273: 1013 1/0/0 A 216.58.194.196 (48)
2016-09-22 23:00:53.809602 IP google-public-dns-a.google.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.33273: 44211 1/0/0 AAAA 2607:f8b0:4005:801::2004 (60)
2016-09-22 23:01:07.096676 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.21176: 33918 1/1/0 CNAME android.l.google.com., (138)
2016-09-22 23:01:07.162773 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.62355: 865 2/0/0 CNAME android.l.google.com., A 216.58.195.78 (84)
2016-09-22 23:01:07.847450 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.15833: 2999 2/0/0 CNAME googleapis.l.google.com., AAAA 2607:f8b0:4005:804::200a (98)
2016-09-22 23:01:07.859860 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.65324: 60161 2/0/0 CNAME googleapis.l.google.com., AAAA 2607:f8b0:4005:807::200a (106)
2016-09-22 23:01:07.878729 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.32663: 64100 6/0/0 CNAME googleapis.l.google.com., A 216.58.195.234, A 172.217.5.106, A 216.58.194.170, A 216.58.195.74, A 216.58.194.202 (150)
2016-09-22 23:01:07.902883 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.25600: 22747 5/0/0 CNAME googleapis.l.google.com., A 216.58.194.170, A 216.58.195.74, A 216.58.194.202, A 172.217.5.106 (142)
2016-09-22 23:01:29.075304 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.61234: 55261 1/1/0 CNAME production-mobile-lb-1918289095.us-east-1.elb.amazonaws.com., (192)
2016-09-22 23:01:29.101026 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.45772: 29888 9/0/0 CNAME production-mobile-lb-1918289095.us-east-1.elb.amazonaws.com., A 52.200.86.130, A 54.88.112.29, A 107.23.72.47, A 54.236.215.162, A 52.1.62.13, A 54.208.76.171, A 52.20.234.99, A 54.209.35.55 (235)
2016-09-22 23:01:35.703399 IP resolver1.opendns.com.domain > c-73-202-157-15.hsd1.ca.comcast.net.45772: 29888 9/0/0 CNAME production-mobile-lb-1918289095.us-east-1.elb.amazonaws.com., A 52.200.86.130, A 54.88.112.29, A 107.23.72.47, A 54.236.215.162, A 52.1.62.13, A 54.208.76.171, A 52.20.234.99, A 54.209.35.55 (235)

HOW DO YOU FIND THAT IN THIS?

Date	Time	Identity	Record Type	Internal IP Address	External IP Address	Action	Destination	Categories
10/24/16	22:00:58	PHW LAN	A	N/A	206.72.10.22	Allowed	connectivitycheck.android.co	Software/Technology
10/24/16	22:00:58	PHW LAN	A	N/A	206.72.10.22	Allowed	lsabc.ikl.com	Business Services
10/24/16	22:00:57	PHWLT18	A	N/A	67.60.9.16	Allowed	remote.connectwise.com	Software/Technology,Allow List
10/24/16	22:00:57	PHWWS34	A	N/A	24.111.168.8	Allowed	wfbs-svc50-en.url.trendmicro	Software/Technology,Allow List
10/24/16	22:00:57	PHW LAN	A	N/A	206.72.10.22	Allowed	android.clients.google.com	Search Engines
10/24/16	22:00:57	PHW LAN	A	N/A	206.72.10.22	Allowed	td.crowdnet.net	Software/Technology,Business Services
10/24/16	22:00:56	PHW LAN	A	N/A	206.72.10.22	Allowed	ad.crowdnet.net	Software/Technology,Business Services
10/24/16	22:00:56	PHW LAN	A	N/A	206.72.10.22	Allowed	dx.weather.com	News/Media,Research/Reference
10/24/16	22:00:56	PHW LAN	A	N/A	206.72.10.22	Allowed	triggers.wfstriggers.com	
10/24/16	22:00:56	PHW LAN	A	N/A	206.72.10.22	Allowed	s.w-x.co	
10/24/16	22:00:55	PHWWS30	A	N/A	206.72.10.22	Allowed	comserver.global.mspa.n-abi	Business Services,Allow List
10/24/16	22:00:55	PHW LAN	A	N/A	206.72.10.22	Allowed	nativeads.mparticle.com	
10/24/16	22:00:54	PHW LAN	A	N/A	206.72.10.22	Allowed	config2.mparticle.com	
10/24/16	22:00:54	PHWWS30	A	N/A	206.72.10.22	Allowed	wfbs-svc50-en.url.trendmicro	Software/Technology,Allow List
10/24/16	22:00:53	PHWWS46	A	N/A	24.111.168.8	Allowed	news.encyclopedia.com	Software/Technology,Business Services
10/24/16	22:00:52	PHW LAN	A	N/A	206.72.10.22	Allowed	adg59.com	Software/Technology,Business Services
10/24/16	22:00:51	PHWWS25	A	N/A	206.72.10.22	Allowed	voisbc.packet8.net	Software/Technology
10/24/16	22:00:51	PHW LAN	A	N/A	206.72.10.22	Allowed	e.crashlytics.com	Software/Technology
10/24/16	22:00:50	PHWWS39	A	N/A	67.60.9.16	Allowed	comserver.global.mspa.n-abi	Business Services,Allow List
10/24/16	22:00:48	PHWLT08	A	N/A	24.111.168.8	Allowed	gv.symcd.com	Software/Technology
10/24/16	22:00:48	PHWLT08	AAAA	N/A	24.111.168.8	Allowed	adadvisor.net	Business Services
10/24/16	22:00:48	PHWLT08	A	N/A	24.111.168.8	Allowed	adadvisor.net	Business Services
10/24/16	22:00:48	PHWLT08	A	N/A	24.111.168.8	Allowed	adadvisor.net	Business Services
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	d.agkn.com	
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	d.agkn.com	
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	d.agkn.com	
10/24/16	22:00:47	PHWLT08	AAAA	N/A	24.111.168.8	Allowed	su.addthis.com	Software/Technology
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	su.addthis.com	Software/Technology
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	su.addthis.com	Software/Technology
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	seg-server-ib.global.prod1.sharethis.net	
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	t.sharethis.com	Social Networking,Software/Technology,Business Services
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	sb.sconeardresearch.com	Business Services
10/24/16	22:00:47	PHWLT08	A	N/A	24.111.168.8	Allowed	seg.sharethis.com	Social Networking,Software/Technology,Business Services
10/24/16	22:00:46	PHWLT08	A	N/A	24.111.168.8	Allowed	httplogserver-ib.global.prod1.sharethis.net	
10/24/16	22:00:46	PHWLT08	A	N/A	24.111.168.8	Allowed	l.sharethis.com	Social Networking,Software/Technology,Business Services
10/24/16	22:00:45	PHW LAN	A	N/A	206.72.10.22	Allowed	analytics.localytics.com	
10/24/16	22:00:45	PHWLT09	A	N/A	24.111.168.8	Allowed	wfbs-svc-nabu-aal.trendmicro	Software/Technology,Allow List
10/24/16	22:00:45	PHW LAN	A	N/A	206.72.10.22	Allowed	shared.iad.apoboy.com	

OR THIS?

comserver.global.msps.able.com	326
s.gyco.b.yahoodns.net	219
wfbs-svc50-en.url.trendmicro.com	166
safebrowsing.google.com	158
s.yimg.com	136
sb.l.google.com	116
safebrowsing-cache.google.com	113
remote.connectwise.com	104
wfbsvc51.lcr.trendmicro.com	102
safebrowsing-cache.Lepotele.com	101
star-mini.c10r.facebook.com	101
star.c10r.facebook.com	100
wfbs-svc-nabu-aal.trendmicro.com	82
espn.hb.omtrdc.net	79
rtmp.tcp.uc.8x8.com	78
www.facebook.com	71
www.amazon.com	68
www.google.com	66
nexus.officeapps.live.com	59
vodsb.packet8.net	59
lt500.tritondigital.com	58
shavar.services.mozilla.com	58
fd-geoycpl-uno.gycpl.b.yahoodns.net	56
labc.8x8.com	55
labc.packet8.net	55
is-comet.albo.01.yahoodns.net	54
is-comet.albo.01.yahoodns.net	54
shavar.prod.mozaws.net	54
geo-um.btril.com	49
meraki.com	45
sb.scorecardresearch.com	43
settings-win.data.microsoft.com	42
mg.mail.yahoo.com	39
vortex-win.data.microsoft.com	37
s.lmgsynd.com	35
www.deltafaucet.com	35
nexusrules.officeapps.live.com	34
0-edge-chat.facebook.com	33
secure-us.lmrworldwide.com	33
or.comet.yahoo.com	32

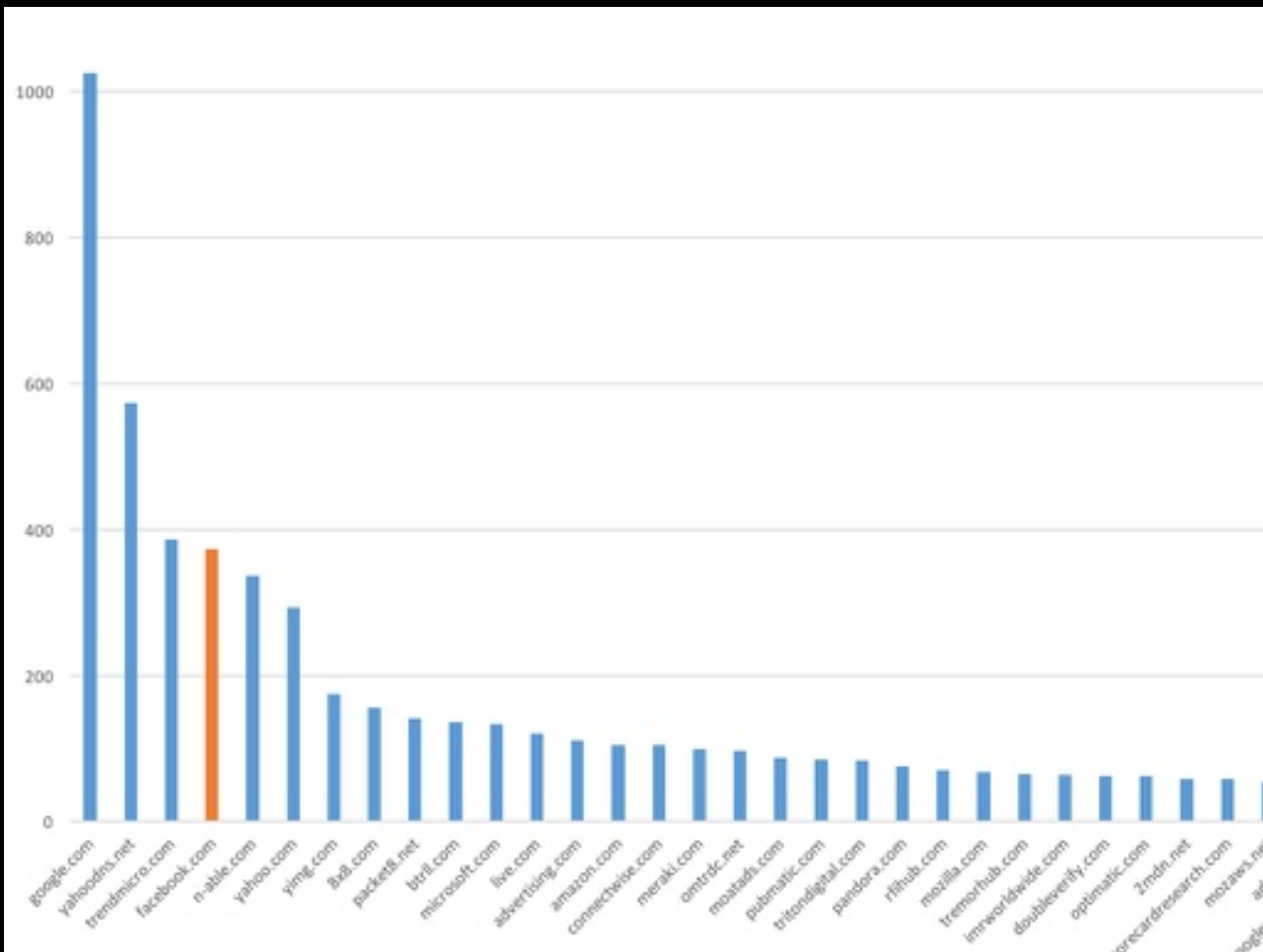
Demonstration on finding popular domains



star-mini.c10r.facebook.com	101
star.c10r.facebook.com	100
www.facebook.com	71
0-edge-chat.facebook.com	33
atlas.c10r.facebook.com	12
connect.facebook.net	11
mqtt.c10r.facebook.com	10
staticxx.facebook.com	10
z-m.c10r.facebook.com	10
pixel.facebook.com	6
instagram.c10r.facebook.com	3
liverail.c10r.facebook.com	3
api.facebook.com	2
error.facebook.com	2
graph.facebook.com	2
m.facebook.com	2
1-edge-chat.facebook.com	1
5-edge-chat.facebook.com	1
b-api.facebook.com	1
b-graph.facebook.com	1
edge-mqtt.facebook.com	1

Counting number of queries





Remove 'Normal'



A	B
360yield.com	1
4finance.com	1
accuweather.com	1
addoox.net	1
adforgecdn.com	1
adingo.jp	1
adition.com	1
adjust.com	1
adlucent.com	1
admantx.com	1
adtechjp.com	1
aim.com	1
akamai.com	1
alfdt.com	1
amcnetworks.com	1
americanexpress.com	1
americangrit.com	1



masterbrand.com mathads.com

mdswanson.com medicaresupplement.com

Manually analyzing a small set of domains

msftncsi.com mshcdn.com myfonts.net

myvzw.com newsinc.com nexage.com

nextadvisor.com norcraftcompanies.com

notanpest.net obtrk.xyz office.net

mathads.com

mdswanson.com medicaresupplement.com

metanetwork.net

mhthemes.com

ministerial5.com

mom.me

monarchads.com mrsteam.com

msftncsi.com mshcdn.com

myvzw.com

notanpest.net obtrk.xyz

medicaresupplement.com

ministerial5.com

mom.me

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz



medicaresupplement.com

ministerial5.com

mom.me

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz



~~medicaresupplement.com~~

ministerial5.com

mom.me

msftncsi.com

myvzw.com

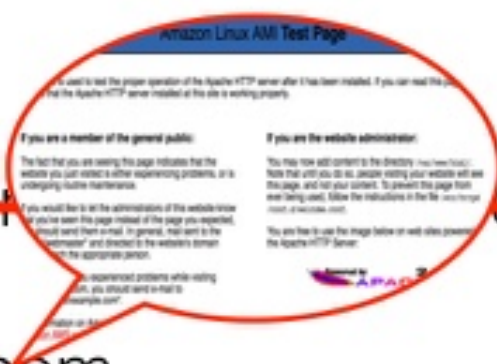
notanpest.net obtrk.xyz

~~medical5.com~~

ministerial5.com
mom.me

msftncsi.com
myvzw.com

notanpest.net obtrk.xyz



~~medicares~~

ministerial5.com

mom.me



Red Wine Steak and
Mushrooms Recipe

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

~~medicares~~

ministerial5.com

~~mom.me~~



Red Wine Steak and
Mushrooms Recipe

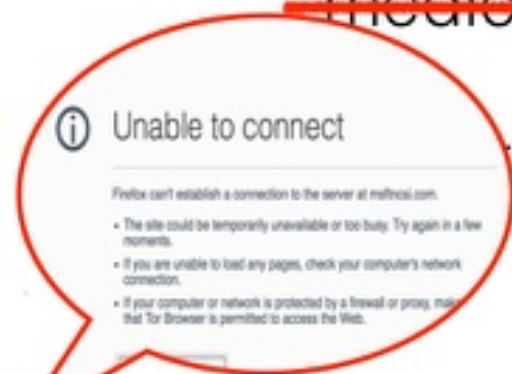
by [author]

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~



.com

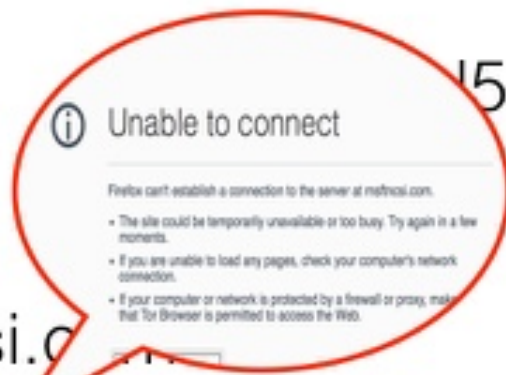
~~mem.me~~

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~



15.com

~~mom.me~~

msftncsi.c

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

ministerial5.com

~~mem.me~~

Forbidden

You don't have permission to access / on this server.

msf

myv2

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

ministerial5.com

~~mom.me~~

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz



ministerial5.com

Latest detected URLs

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

1/61	2014-12-05 01:07:21	http://ministerial5.com/
------	---------------------	---

ministerial5.com

Ministerial5 - SonicWALL Security Center

software.sonicwall.com/applications/app/index.asp?ev=appd...app...**Ministerial5** ▼

Application: Ministerial5. This domain used by an advertising company that is part of a network of sites, cookies, and other technologies used to track you, what ...

~~medicaresupplement.com~~

ministerial5.com

~~mom.me~~

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

What is www.msftncsi.com? - Knowledge eXchange

<https://kx.cloudingenium.com/microsoft/servers/windows.../what-is-www-msftncsi-co...> ▼

Mar 20, 2014 - This is because the url www.msftncsi.com is generally used by Windows machines to verify that there is network connectivity. A Windows ...

msftncsi.com

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

msftncsi.com

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

~~msftncsi.com~~

myvzw.com

notanpest.net obtrk.xyz

12-20-2011, 12:58 AM

(Stephen) ○

Owner of the net for a day

that is verizon phones network.

Someone maybe using that LTE to spam 😊

myvzw.com

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

~~msftncsi.com~~

myvzw.com

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

~~msftncsi.com~~

~~myvzw.com~~

notanpest.net obtrk.xyz

Domain > obtrk.xyz | Threatcrowd.org Open Source Threat Intelligence

<https://www.threatcrowd.org/domain.php?domain=obtrk.xyz> ▼

Domain > obtrk.xyz. × Welcome! Right click nodes and scroll the mouse to navigate the graph. Is this malicious? Yes No. Whois Details. Property, Value.

obtrk.xyz

obtrk.xyz domain information

Passive DNS replication

VirusTotal's passive DNS only stores address records. This domain has been seen to resolve to the following IP addresses.

2016-08-16 174.139.202.5

Latest undetected files that embed this domain in their strings

Latest files that are not detected by any antivirus solution and embed URL pattern strings with the domain provided.

0/56	fc04d2a728f44579ea346d50400bf2c01b68b990960a1b7425f2dee623c71748
0/56	ecf816a097e4387f7a2d9f275097c4896026482f6ebb059edceba2bb193a6ea5
0/53	0387a453e2205e4cf0a869c0165d76577da874070d034a8ba8c8e217a46fab9e
0/55	f4f911cf1ff62f109500f100c0920ddb26948e1d57481c00dcc44ea86b21ceb9

obtrk.xyz

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

~~msftncsi.com~~

~~myvzw.com~~

notanpest.net obtrk.xyz

~~medicaresupplement.com~~

~~ministerial5.com~~

~~mom.me~~

~~msftncsi.com~~

~~myvzw.com~~

notanpest.net ~~obtrk.xyz~~

notanpest.net

Malwr - Malware Analysis by Cuckoo Sandbox

<https://malwr.com/.../NDAxMWNkZjNmODhINDgwMDhkMTFIZmYwZDFjMTg4O...> ▼

1 day ago - WinHttpRequest.5)', u'method': u'GET', u'host': u'notanpest.net', u'version': u'1.1', u'path': u'/0d2fo', u'data': u'GET /0d2fo HTTP/1.1\r\nAccept: ...

budget_xls_f20e62f27.zip - Free Automated Malware Analysis Service ...

<https://www.hybrid-analysis.com/.../aa81c35df01e6b92c0279c2a7d76662c231ab5688c...>

14 hours ago - NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; http://notanpest.net/3cglmvsj, malicious, 2/68, 10/25/2016 10:40:56, -. Associated ...

File Details - Free Automated Malware Analysis Service - powered by ...

<https://www.hybrid-analysis.com/.../4b6aea83a2bc928383b9209c0c72dbef2a48071146...>

1 day ago - Endpoint, Method/Response, URL/Code, Data. 67.171.65.64:80 (notanpest.net), GET, /68ehx, GET /68ehx HTTP/1.1 Connection: Keep-Alive ...

notanpest.net

Malwr - Malware Analysis by Cuckoo Sandbox

<https://malwr.com/.../NDAXMWNkZjNmODhINDgwMDhkMTFIZmYwZDFjMTg4O...> ▼

1 day ago - WinHttpRequest.5)', u'method': u'GET', u'host': u'notanpest.net', u'version': u'1.1', u'path': u'/0d2fo', u'data': u'GET /0d2fo HTTP/1.1\r\nAccept: ...

budget_xls_f20e62f27.zip - Free Automated Malware Analysis Service ...

<https://www.hybrid-analysis.com/.../aa81c35df01e6b92c0279c2a7d76662c231ab5688c...>

14 hours ago - NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; http://notanpest.net/3cgImvsj, malicious, 2/68, 10/25/2016 10:40:56, -. Associated ...

File Details - Free Automated Malware Analysis Service - powered by ...

<https://www.hybrid-analysis.com/.../4b6aea83a2bc928383b9209c0c72dbef2a48071146...>

1 day ago - Endpoint, Method/Response, URL/Code, Data. 67.171.65.64:80 (notanpest.net), GET, /68ehx, GET /68ehx HTTP/1.1 Connection: Keep-Alive ...

notanpest.net

File has been identified by at least one AntiVirus on VirusTotal as malicious

Performs some HTTP requests

Steals private information from local Internet browsers

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Installs itself for autorun at Windows startup

notanpest.net

⚠ Latest detected URLs

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

3/68	2016-10-25 23:18:36	http://notanpest.net/
4/68	2016-10-25 15:22:53	<u>http://notanpest.net/68ehx</u>
4/68	2016-10-25 15:22:43	<u>http://notanpest.net/3cglmvsj</u>
4/68	2016-10-25 15:22:34	<u>http://notanpest.net/0d2fo</u>
4/68	2016-10-25 15:22:28	<u>http://notanpest.net/214t44m0</u>

notanpest.net

DETAILS FOR NOTANPEST.NET

This domain is currently in the OpenDNS Security Labs block list

This domain has a suspicious ASN score

This domain has a suspicious prefix score

Classifier prediction: suspicious

OpenDNS Security Graph Score: **100**

Geo distance between hosts serving this domain is fairly high



notanpest.net

That Process is...
Really Tedious



Tiring

- Mostly Manual
- Requires Expertise



The Solution?



AUTOMATION



Program Ourselves out of a Job

What do we Automate?

- Auto-Clean Logs and Network Streams
- Auto-Process
- Find ways to remove 'normal'
- Categorization
- Save to a workable whatever
- Visualization



Auto-Clean Logs and Network Streams

It's all different



Auto-Clean Logs and Network Streams

- DNS

```
2017-01-18T11:21:44-05:00 daemon prod named[16648]: info client 10.36.64.10#35225 (www.ges.ca): query: www.ges.ca IN A +EDC (10.210.210.35)
```

```
2017-05-02 08:56:44,webservices.prime.com,A,208.91.197.27
```



Auto-Clean Logs and Network Streams

- DNS
- Active Directory

```
Subject:
  Security ID:      SYSTEM
  Account Name:     DC03$
  Account Domain:   AD
  Logon ID:         0x1b2623ae

Logon Type:        3

This event is generated when a logon session is destroyed. It may be positively correlated with the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Audit Success,10/26/2016 10:15:37 AM,Microsoft-Windows-Security-Auditing,4624,Logon Succeeded on.

Subject:
  Security ID:      NULL SID
  Account Name:     -
  Account Domain:   -
  Logon ID:         0x0

Logon Type:        3

New Logon:
  Security ID:      SYSTEM
  Account Name:     DC03$
  Account Domain:   AD
  Logon ID:         0x1b2623ae
  Logon GUID:       {44F7D735-74A2-6B4C-0AE3-9969F562CFB0}
```



Auto-Clean Logs and Network Streams

- DNS
- Active Directory
- System

```
Sep 12 06:39:01 evl CRON[17316]: pam_unix(cron:session): session closed for user root
Sep 12 07:09:01 evl CRON[17340]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 07:09:01 evl CRON[17340]: pam_unix(cron:session): session closed for user root
Sep 12 07:17:01 evl CRON[17364]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 07:17:01 evl CRON[17364]: pam_unix(cron:session): session closed for user root
Sep 12 07:39:01 evl CRON[17369]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 07:39:01 evl CRON[17369]: pam_unix(cron:session): session closed for user root
Sep 12 08:09:01 evl CRON[17393]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 08:09:01 evl CRON[17393]: pam_unix(cron:session): session closed for user root
Sep 12 08:17:01 evl CRON[17415]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 08:17:01 evl CRON[17415]: pam_unix(cron:session): session closed for user root
Sep 12 08:39:01 evl CRON[17420]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 08:39:01 evl CRON[17420]: pam_unix(cron:session): session closed for user root
Sep 12 09:09:01 evl CRON[17444]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 09:09:01 evl CRON[17444]: pam_unix(cron:session): session closed for user root
Sep 12 09:15:43 evl sshd[17466]: Bad protocol version identification 'GET / HTTP/1.1' from 94.136.145.178 port 40776
```



Auto-Clean Logs and Network Streams

- DNS
- Active Directory
- System
- HTTP

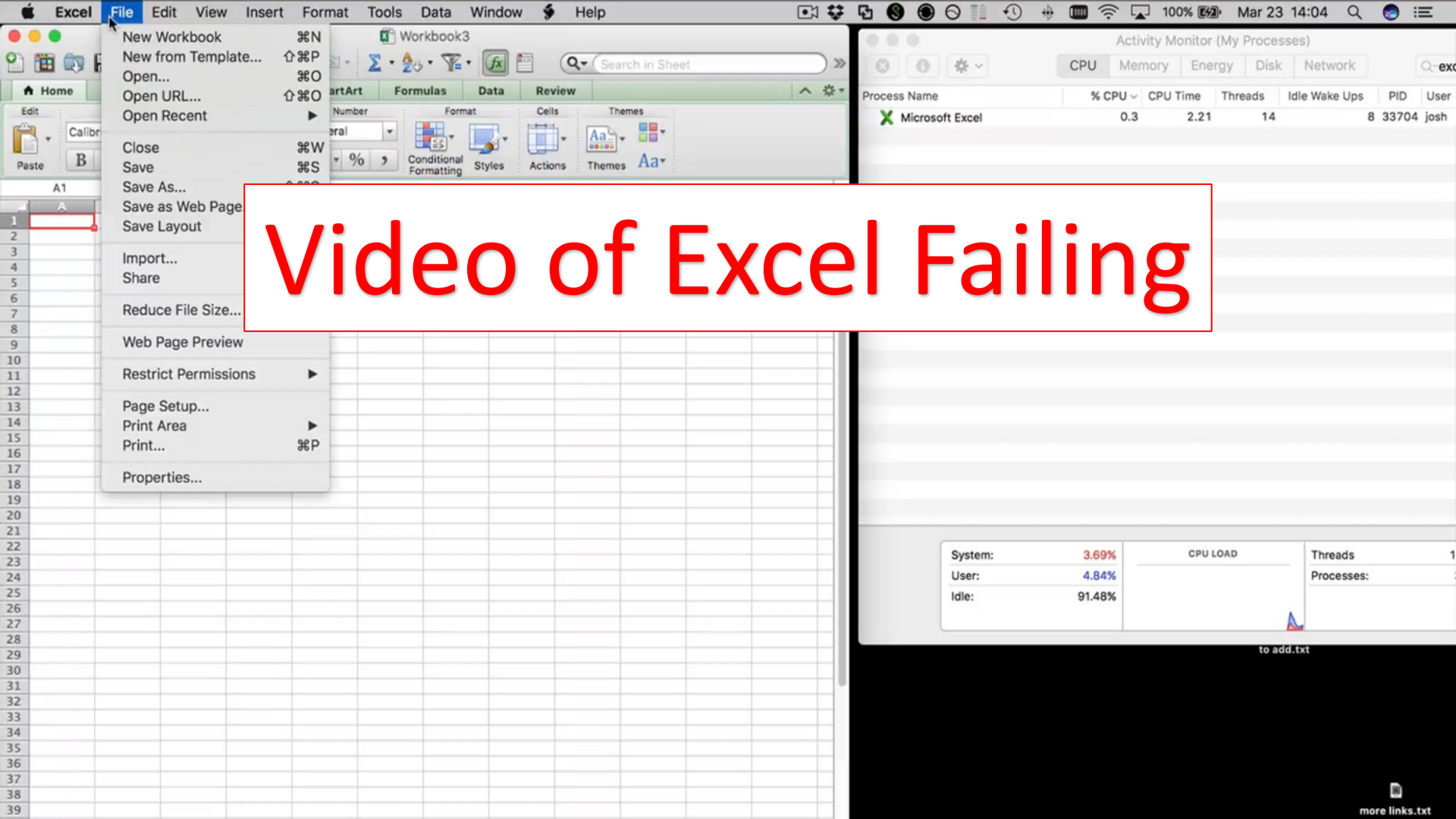
```
absentfaith.com:443 207.46.13.161 - - [09/May/2017:06:49:25 -0700] "GET / HTTP/1.1" 200 21632 "-" "Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)"
absentfaith.com:80 34.202.166.20 - - [09/May/2017:06:50:32 -0700] "HEAD /wp-login.php HTTP/1.1" 301 175 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-us; rv:1.7.12) Gecko/20050919 Firefox/1.0.7"
65.19.134.142:80 180.76.15.23 - - [09/May/2017:06:58:25 -0700] "GET /robots.txt HTTP/1.1" 301 443 "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"
65.19.134.142:80 180.76.15.26 - - [09/May/2017:06:58:26 -0700] "GET /robots.txt HTTP/1.1" 301 443 "-" "Mozilla/5.0 (Windows NT 5.1; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"
65.19.134.142:80 180.76.15.5 - - [09/May/2017:06:59:06 -0700] "GET / HTTP/1.1" 301 423 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
evol13.com:443 180.76.15.30 - - [09/May/2017:06:59:07 -0700] "GET / HTTP/1.1" 200 3476 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
absentfaith.com:443 180.76.15.23 - - [09/May/2017:07:10:08 -0700] "GET /?m=20010718 HTTP/1.1" 200 36797 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
absentfaith.com:443 66.249.79.123 - - [09/May/2017:07:10:21 -0700] "GET /robots.txt HTTP/1.1" 404 3631 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
absentfaith.com:443 66.249.79.123 - - [09/May/2017:07:10:21 -0700] "GET /?m=200506 HTTP/1.1" 200 7734 "-" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
jpyorre.com:80 180.76.15.162 - - [09/May/2017:07:12:19 -0700] "GET / HTTP/1.1" 301 427 "-" "Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)"
```



Auto-Process

The manual way needs to go away





Video of Excel Failing

Auto-Process

- Use what makes sense to you
 - ~~Excel~~



Auto-Process

- Use what makes sense to you

- ~~Excel~~
- R



Auto-Process

- Use what makes sense to you

- ~~Excel~~

- R

- Python

Matplot, Pandas, Plotly, D3, C3, etc...



Tools (Open Source)

- pyasn (offline ASN lookup)



Tools (Open Source)

- pyasn (offline ASN lookup)

```
Macbook-Pro-Home:app josh$ python tester.py 1000.txt
```

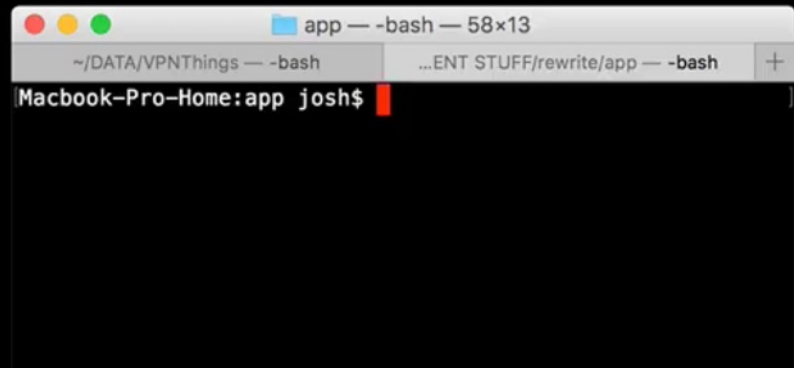
Demo of PYASN



Tools (Open Source)

- pyasn (offline ASN lookup)
- python whois
- NetworkX





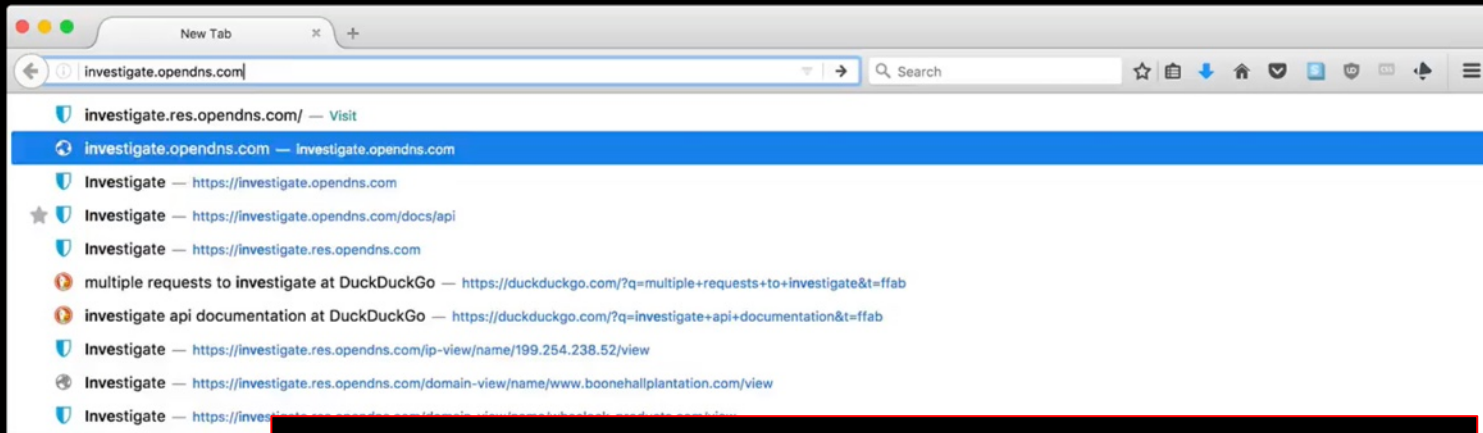
Demo of PYASN and NetworkX



Tools (Paid)

- OpenDNS Investigate





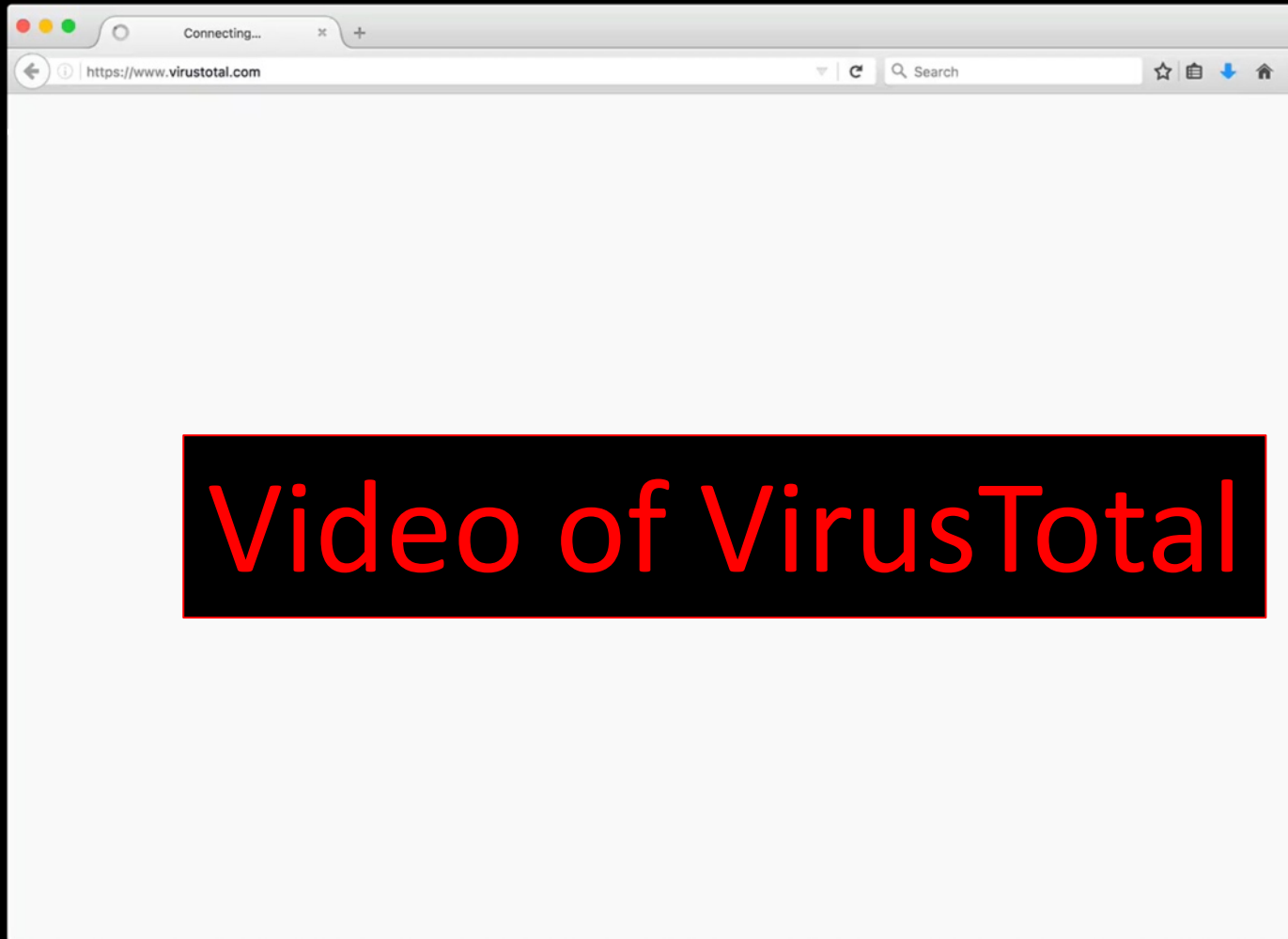
Video of Investigate



Tools (Paid)

- OpenDNS Investigate
- VirusTotal





Find ways to remove 'normal'

- Creating a Baseline
 - Count things and remove 'Popular'



Find ways to remove 'normal'

- Start with data from OpenDNS
- Approx 3% of the internet
- How do you find normal?
- Can you find normal?



```
evol13:logs josh$ wc -l 2016-08-25-17-20.myzPMsaJ
664938 2016-08-25-17-20.myzPMsaJ
evol13:logs josh$ |
```

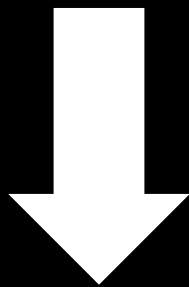
Video of Raw Log File

Let's Try Anyway

- Count how many times a domain is queried
 - Over 10 times: Write to normal_traffic.txt
 - Under 3 times: Write to suspicious_traffic.txt



08/25/2016 17:20:00, s1.mohito.com, A, 360, 78.24.161.76







08/25/2016 17:29:00, hotspotcostablanca.ath.cx, A, 60, 81

9 Minutes



```
wc -l 2016-08-25-17-20.myzPMsaJ  
664,938 2016-08-25-17-20.myzPMsaJ
```



	2016-08-25-17-20.myzPMsaJ	Aug 25, 2016, 10:32 AM	61.3 MB
	clean_data_opendnsquerylog.py	Today, 11:09 AM	3 KB
	normal_traffic.txt	Today, 11:10 AM	247 KB
	suspicious_traffic.txt	Today, 11:10 AM	6.4 MB



'Normal' Traffic

clients.l.google.com	8687
www.google.com	7145
youtube-ui.l.google.com	2820
www-google-analytics.l.google.com	2196
sb.l.google.com	2190
yting.l.google.com	2118
safebrowsing.cache.l.google.com	2031
gstaticadssl.l.google.com	1903
plus.google.com	1641
plus.l.google.com	1572
play.l.google.com	1300
video-stats.l.google.com	1224
gateway.push-apple.com.akadns.net	1062
2.android.pool.ntp.org	1053
www3.l.google.com	1053



'Suspicious' Traffic

test.url.dnsdun.com	3
elb039497-690954886.us-east-1.elb.amazonaws.com	3
images.infospace.com	3
pervert.engdecision.com	3
r5---sn-25ge7nlz.googlevideo.com	3
recon.bleacherreport.com	3
winestyle.ru	3
q23.queuev4.vk.com	3
tf-lb-5xcuvnk75jgj3bkuhud4qg7tli-1336305397.eu-west-1.elb.amazonaws.com	3
r1.sn-3c27ln7k.googlevideo.com	3
elb040935-2033726180.us-east-1.elb.amazonaws.com	3
customers.anpdm.com	3
exmail-eu1.chevron.com	3
men.ru	3



DETAILS FOR WINESTYLE.RU

Classifier prediction: benign

OpenDNS Security Graph Score: **+100**

According to the requester geo distribution, this domain is very likely to be benign

Still under development

****EXPERIMENTAL**** OpenDNS Security Graph Score: **94** ?

DNS queries



★★★★★
Гарантия качества и
безопасности

Оригинальные продукты от
официальных импортеров. Продажи под
контролем ЕГАИС

Тысячи отзывов и оценок реальных
покупателей. Доверие постоянных
клиентов

WineStyle в списке
крупнейших e-commerce
компаний России

Подробнее



📍 Адреса магазинов

📞 Заказать звонок

Корпоративным клиентам

🔍 WineStyle

En

WineStyle¹⁸⁺

Поиск по каталогу



👤 Личный кабинет



Корзина



Все товары

Вино

Шампанское

Виски

Коньяк

Пиво

Ликер

Гралпа

Вода

Наборы и подарки



Вина до 1000 рублей
С высоким рейтингом

WINE SPECTATOR

ROBERT PARKER

STEVEN TANZER'S

WINE ENTHUSIAST

BEHAVIORAL ANALYSIS USING DNS & NETWORK TRAFFIC



CISCO
OpenDNS

More 'Suspicious' Traffic

mail.exotissimo.com	1
www.erlerlab.com	1
r2---sn-oapm-guhe.gvt1.com	1
weltweitkochen.de	1
appear.ro	1
a-pcisg01sl04.insnw.net	1
web1.arh.noaa.gov	1
ldaviesmorris.orangehome.co.uk	1
www.electriks.co.uk	1
app.vconnect.com	1
sonahay.com	1
ns1.ahcdn.com	1
tsast.kz	1
r6---sn-5hnednez.googlevideo.com	2
rajshreesugars.com	1



DETAILS FOR TSAST.KZ

This domain is currently in the OpenDNS Security Labs block list

Classifier prediction: suspicious

OpenDNS Security Graph Score: **-56**

Still under development

****EXPERIMENTAL**** OpenDNS Security Graph Score: **34** ?

DNS queries



2016/03/30 16:49

BLACK

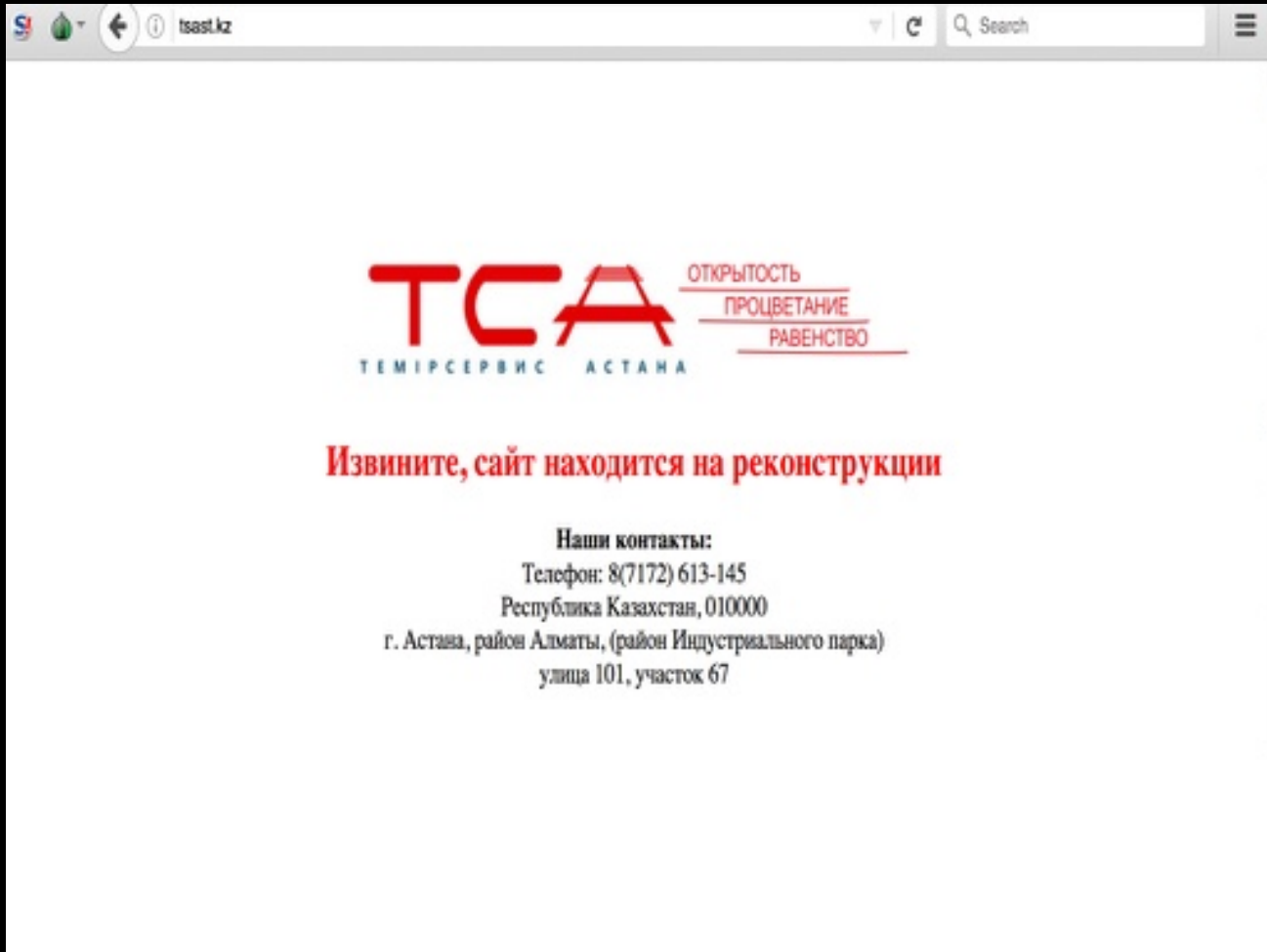
ACTIVE

malware2

Dropper

locky





Find ways to remove 'normal'

- Creating a Baseline
 - Count things and remove 'Popular'
 - Use a 'Top Domains' list





Switch to DuckDuckGo and
take back your privacy!

- 1 We don't store your personal info.
- 2 We don't follow you around with ads.
- 3 We don't track you. Ever.

Add DuckDuckGo to Safari



Video of Top Domain Lists



Find ways to remove 'normal'

- Creating a Baseline
 - Count things and remove 'Popular'
 - Use a 'Top Domains' list

```
top_domains = []  
with open('top-1m.csv', 'r') as td:  
    for line in td:  
        line = line.strip()  
        line = line.split(',')  
        top_domains.append(line[1])
```



Find ways to remove 'normal'






- Creating a Baseline
 - Count things and remove 'Popular'
 - Use a 'Top Domains' list

```
with open(input_file, 'r') as f:
    for line in f:
        domain = line.strip() # get rid of extra blank lines
        if domain in top_domains:
            writefile = open('in_top1m.txt', 'a')
            writefile.write(domain)
            writefile.write('\n')
            writefile.close()
        else:
            writefile = open('not_in_top1m.txt', 'a')
            writefile.write(domain)
            writefile.write('\n')
            writefile.close()
```



Find ways to remove 'normal'

- Creating a Baseline
 - Count things and remove 'Popular'
 - Use a 'Top Domains' list

	top-1m.csv	Apr 10, 2017, 9:57 PM	29.3 MB	Comma...eet (
	2016-08-25-17-20.myzPMsaJ	Aug 25, 2016, 10:32 AM	61.3 MB	Document
	in_top1m.txt	Today, 2:31 PM	599 KB	Plain Text
	not_in_top1m.txt	Today, 2:31 PM	1.4 MB	Plain Text
	clean_data_opendnsquerylog.py	Today, 2:05 PM	5 KB	Python



Find ways to remove 'normal'

- Creating a Baseline
 - Count things and remove
 - Use a 'Top Domains' list

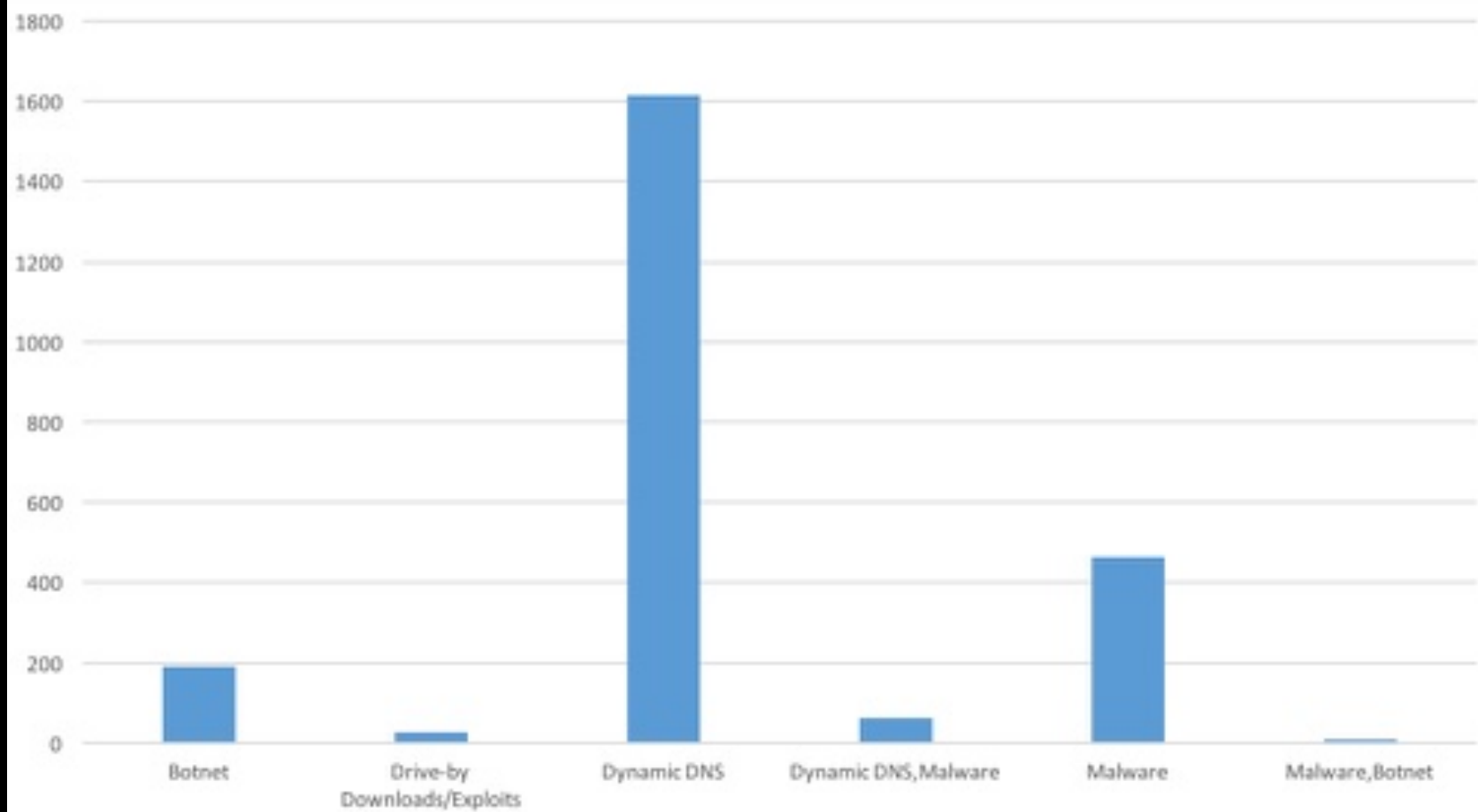
in_top1m.txt		not_in_top1m.txt	
16193	google.co.uk	611	1go.dk
16194	google.co.za	612	1go1e.net
16195	google.com	613	1google.com
16196	google.com.ar	614	1hes.ir
16197	google.com.au	615	1homegift.com
16198	google.com.br	616	1host.gr
16199	google.com.cy	617	1host.kz
16200	google.com.eg	618	1istok.ru
16201	google.com.gh	619	1jm98.com
16202	google.com.gr	620	1jour1surprise.com
16203	google.com.hk	621	1ka.ru
16204	google.com.jm	622	1kapper.nl
16205	google.com.kh	623	1key.nl
16206	google.com.kw	624	1kino.com
16207	google.com.mt	625	1kish.com
16208	google.com.mx	626	1klang.de
16209	google.com.ng	627	1klik.hr
16210	google.com.pk	628	1kssport.com
16211	google.com.ru	629	1luxury039.com



Categorization

- Third Party Service





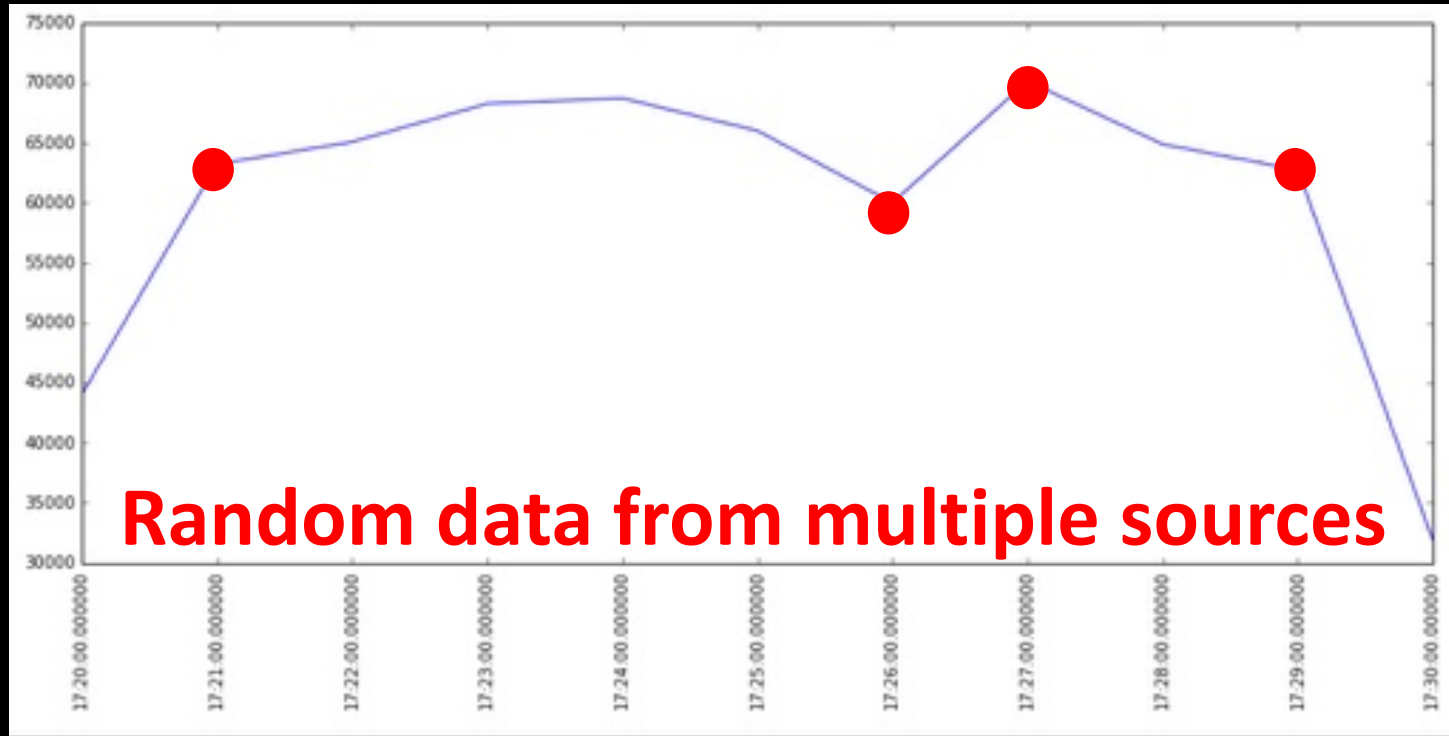


Categorization

- You may need to use multiple third parties



Looking at the Bandwidth



Narrow the Focus



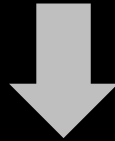
DNS: One Organization

```
wc -l dnsqueries.txt  
19801469 dnsqueries.txt
```



DNS: One Organization

19-May-2015 01:14:36.782



19-May-2015 18:30:29.366




```
evol13:oneorganization josh$ |
```



Video of Log File

DNS: One Organization

 all_dateanddomain.txt

Today, 4:13 PM

875.8 MB



DNS: One Organization

```
cat all_dateanddomain.txt | grep -v directv > slightlycleaned.txt
```

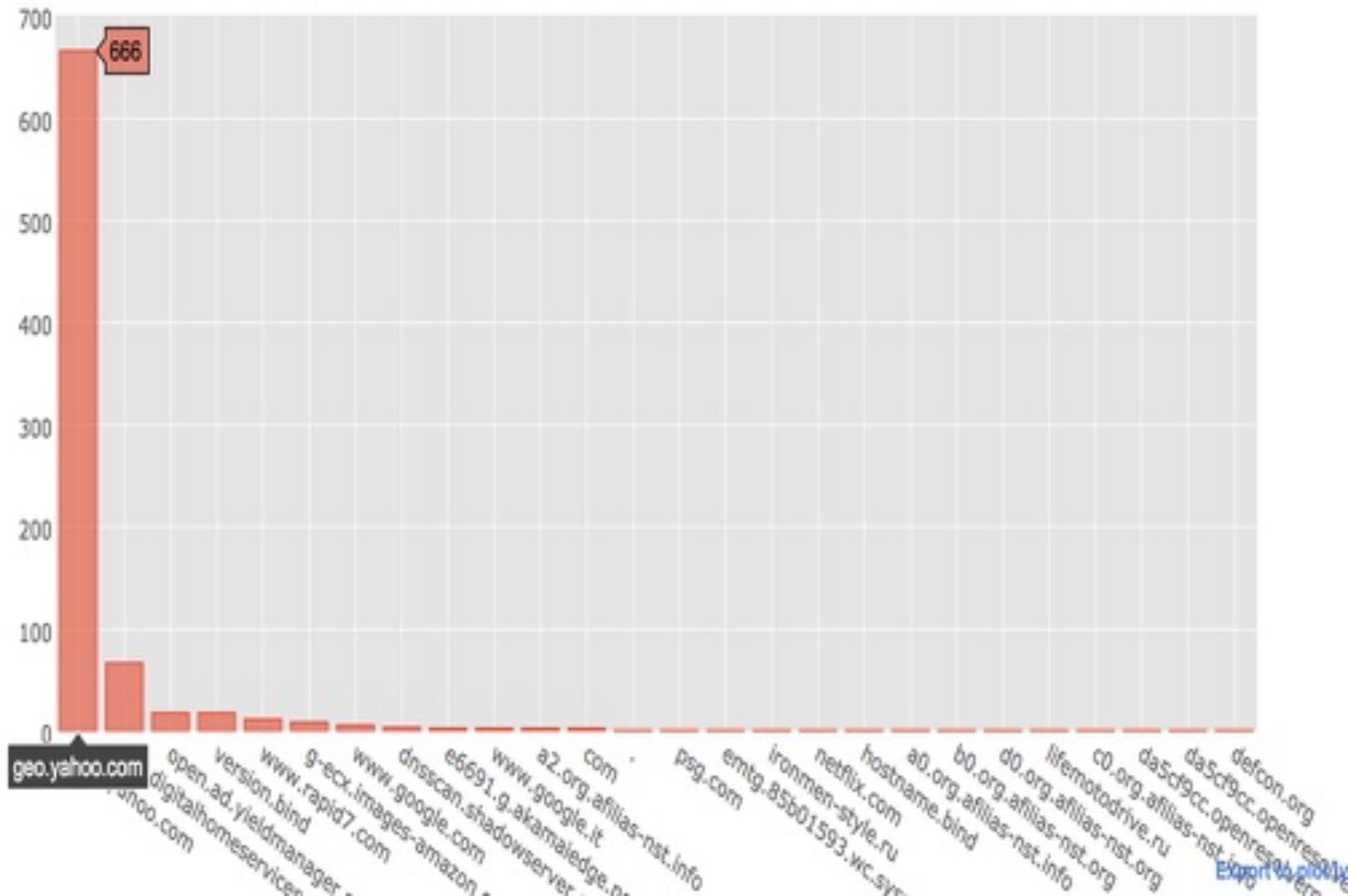
```
wc -l slightlycleaned.txt  
493351 slightlycleaned.txt
```



DNS: One Organization

```
wc -l mindomains.txt  
1320 mindomains.txt
```





DNS: One Organization

2 GB File: Taking forever

```
In [*]: with open('dnsqueries.txt', 'r') as f:  
        df_v2 = map(lambda x: Data(x), f.readlines())
```

Process Name	% CPU ▾	CPU Time	Threads	Idle Wake Ups	PID	User
Python	98.1	11:59.14	13	1	13465	josh



Streaming Data

- Ran this on a system at home:

```
tcpdump -i eth1 -j host port 53 -ttt >> tcpdump.log
```

eth1 is hooked up to a network tap watching traffic between the routers internet port and the cable modem



It looks like this:

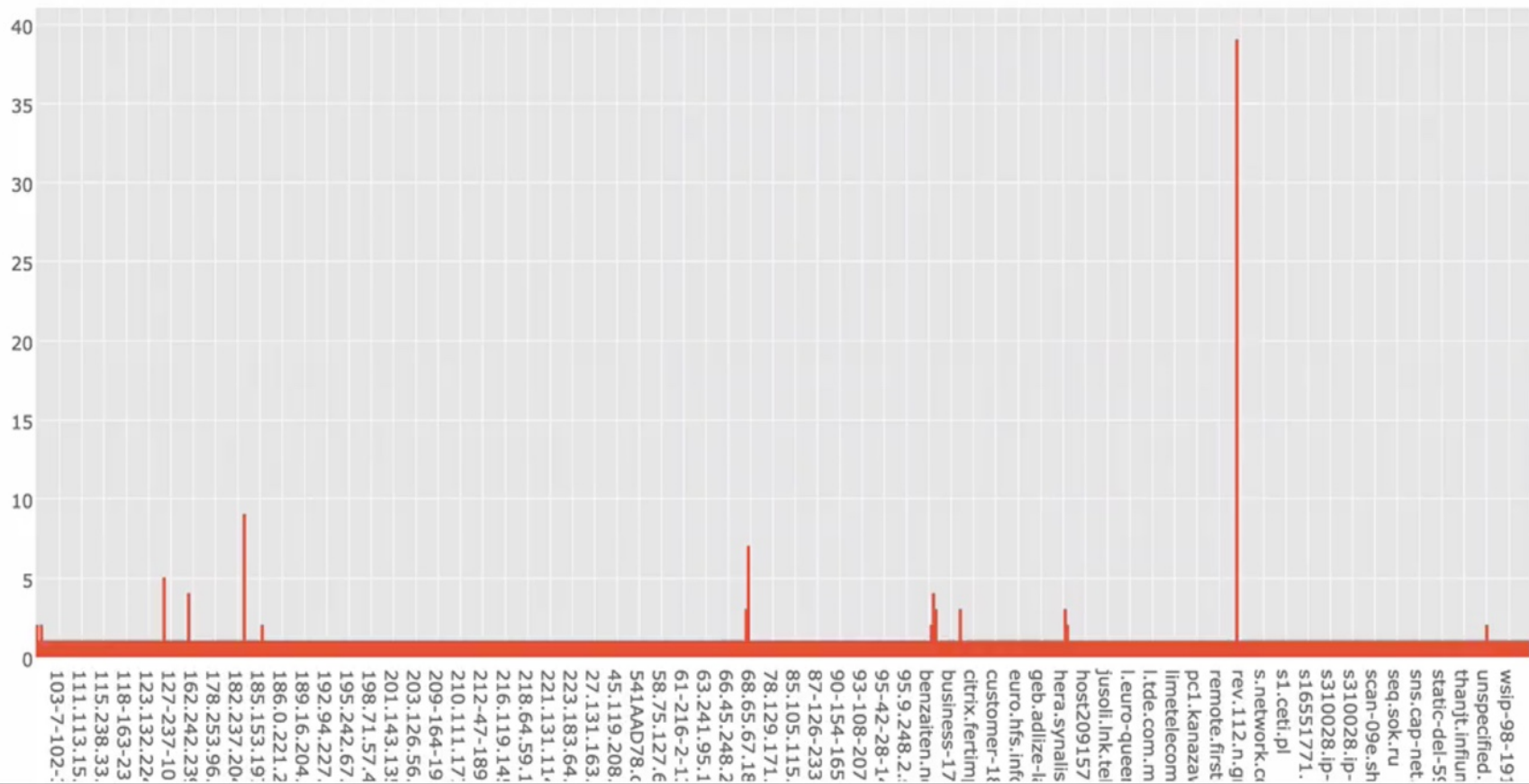
```
12:56:37.854306 IP 73.202.157.15.53018 >
208.67.222.222.53: 46044+ A? apple.com. (27)
E..7..@.@...I....C.....
5.#.w.....apple.com.....
12:56:37.854517 IP 73.202.157.15.2461 >
208.67.222.222.53: 18586+ A? calendar.google.com. (37)
E..A..@.@...I....C.. ..
5.-.xH.....calendar.google.com.....
12:56:37.854681 IP 73.202.157.15.25959 >
208.67.222.222.53: 17850+ A? 1-courier.push.apple.com.
(42)
E..F..@.@...I....C..eg.5.2V.E..... 1-
courier.push.apple.com.....
12:56:37.854906 IP 73.202.157.15.15125 >
208.67.222.222.53: 63415+ A? 14-lvl3-pdl.vimeocdn.com.
(42)
```

It looks like this:

```
12:56:37.854306 IP 73.202.157.15.53018 >
208.67.222.222.53: 46044+ A? apple.com. (27)
E..7..@.@...I....C.....
5.#.w.....apple.com.....
12:56:37.854517 IP 73.202.157.15.2461 >
208.67.222.222.53: 18586+ A? calendar.google.com. (37)
E..A..@.@...I....C.. ..
5.-.xH.....calendar.google.com.....
12:56:37.854681 IP 73.202.157.15.25959 >
208.67.222.222.53: 17850+ A? 1-courier.push.apple.com.
(42)
E..F..@.@...I....C..eg.5.2V.E..... 1-
courier.push.apple.com.....
12:56:37.854906 IP 73.202.157.15.15125 >
208.67.222.222.53: 63415+ A? 14-lvl3-pdl.vimeocdn.com.
(42)
```

2016-10-01 06:44:37.757943	213.248.136.201	1
2016-09-24 20:49:40.088250	198-23-246-106-host.colocrossing.c	1
2016-09-26 03:49:22.371722	unspecified.mtw.ru	1
2016-09-24 03:48:43.992155	185.70.187.212.50961	1
2016-09-24 05:48:26.268283	hosted-by.2sync.co.36004	1
2016-09-25 23:48:12.961130	5.128.19.178.abo.tutor.fr	1
2016-09-30 04:52:23.139389	-gw.e-macro.ne.jp	1
2016-09-30 01:07:03.869564	broadband-77-37-249-161.nationalcablenetworks.ru	1
2016-09-29 06:30:58.196625	secure.plusmatrixdesign.c	1
2016-09-24 22:36:10.109266	s310028.ip-188-165-195.eu.48009	1
2016-09-27 22:53:03.382517	208-58-201-162.c3-0.brae-ubr1.lnh-brae.md.cabl...	1
2016-09-27 18:08:32.607464	195.242.67.20	1
2016-09-26 19:54:09.605774	kl-ftp-mrdns1.ihug.net	1
2016-09-27 23:29:51.476885	208.99.191.136	1
2016-09-28 01:09:34.937425	resolver1.privateinternetaccess.c	1
2016-09-27 10:16:02.064874	s-1.fidelityaccess.net	1
2016-09-28 01:35:47.819020	201.143.135.175.dsl.dyn.telnor.net	1
2016-09-27 18:55:43.041106	124.107.19.227.pldt.net	1
2016-09-24 17:36:03.782716	static-dsl-161.87-197-159.telecom.sk	1

Requests



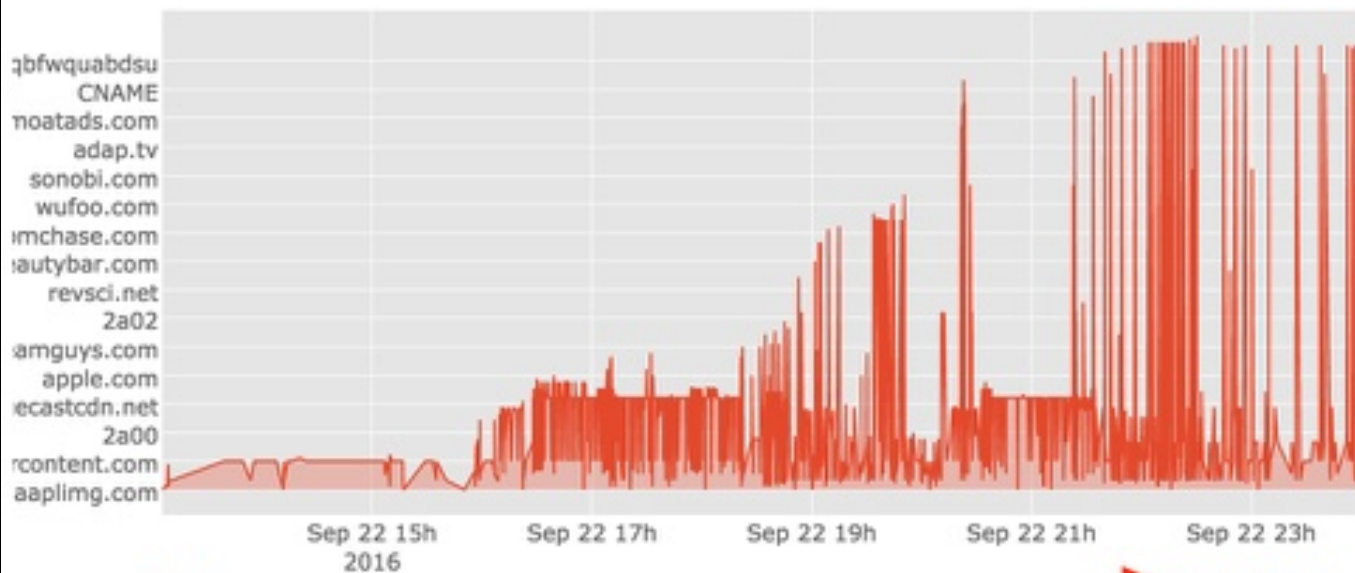


Noticing Suspicious Activity

Comparing Activity



Time Series from 09-22



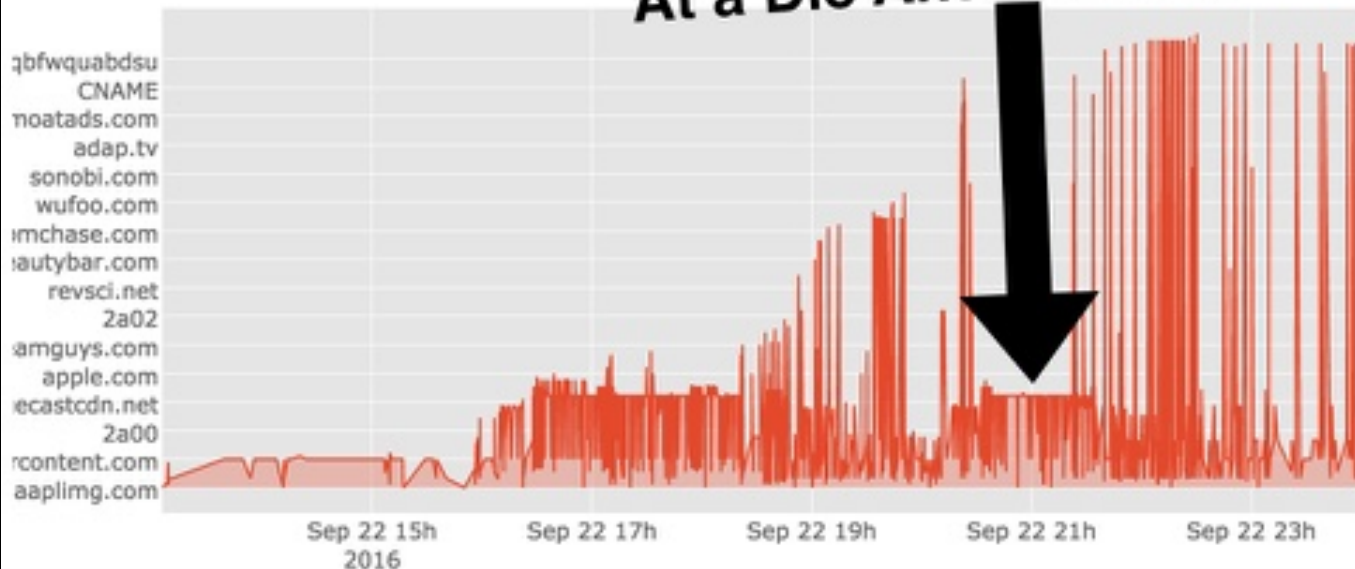
0 hr

24 hr

Thursday

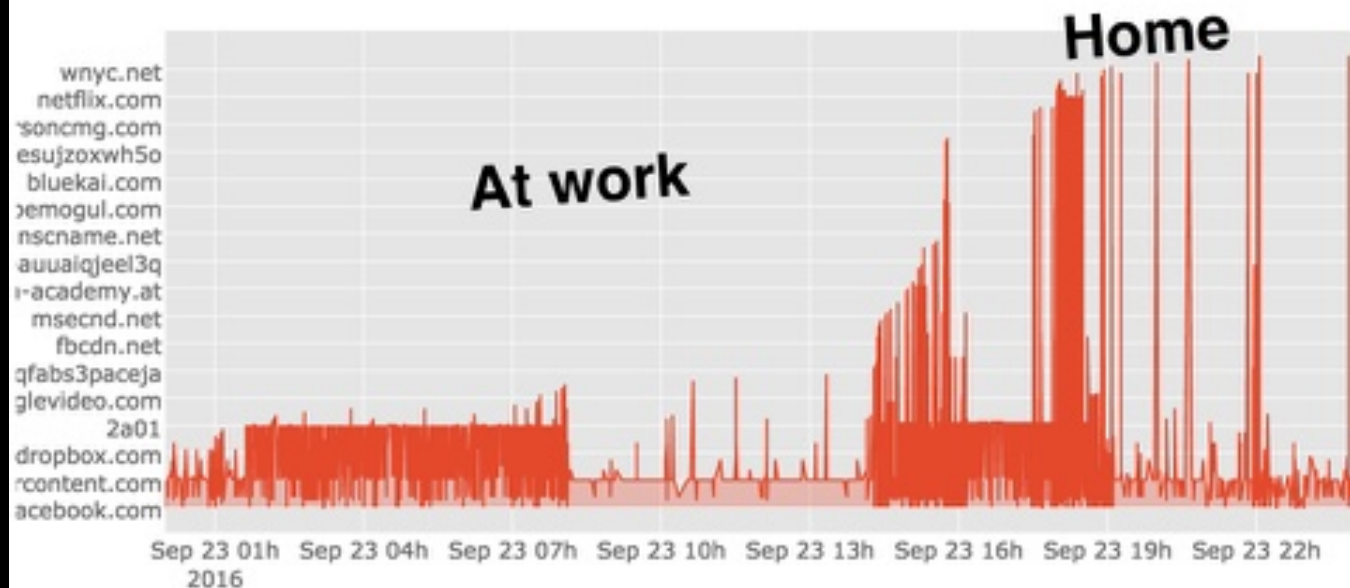
Time Series from 09-22

At a Die Antwoord concert



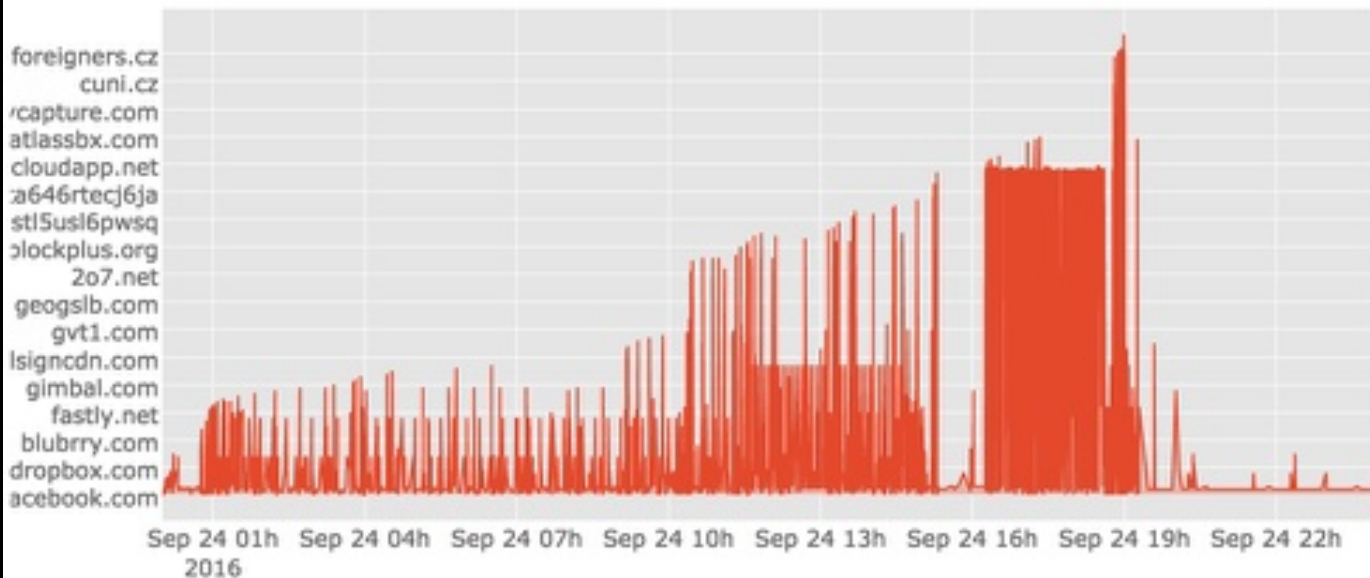
Friday

Time Series from 09-23



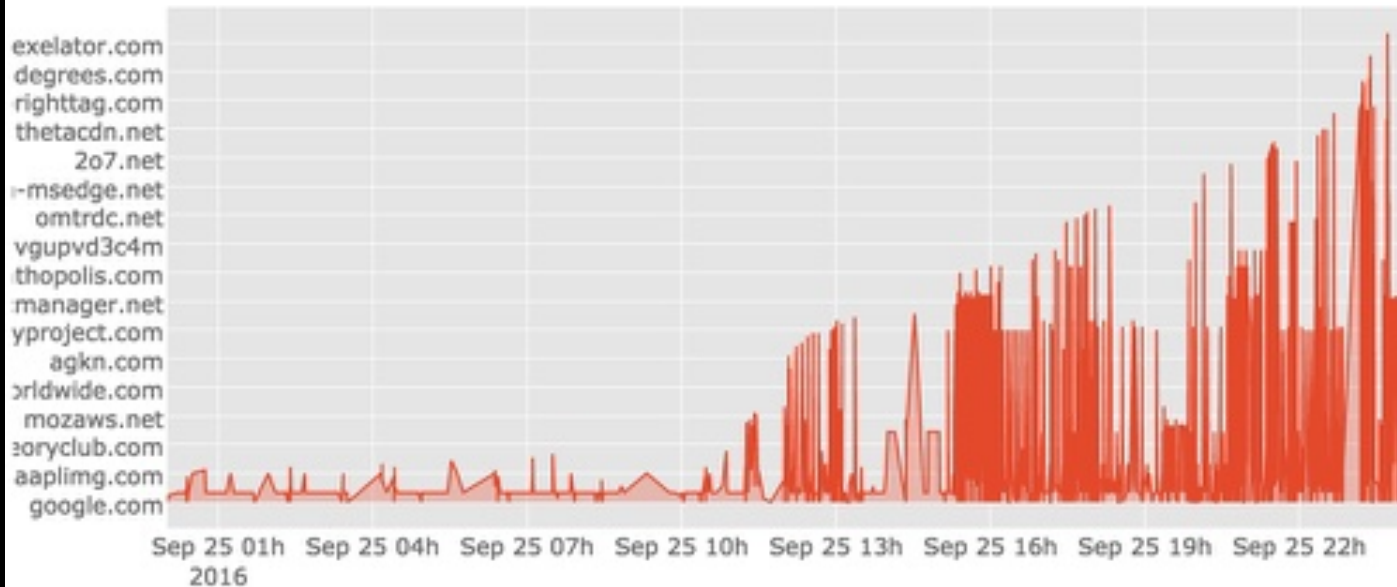
Saturday

Time Series from 09-24



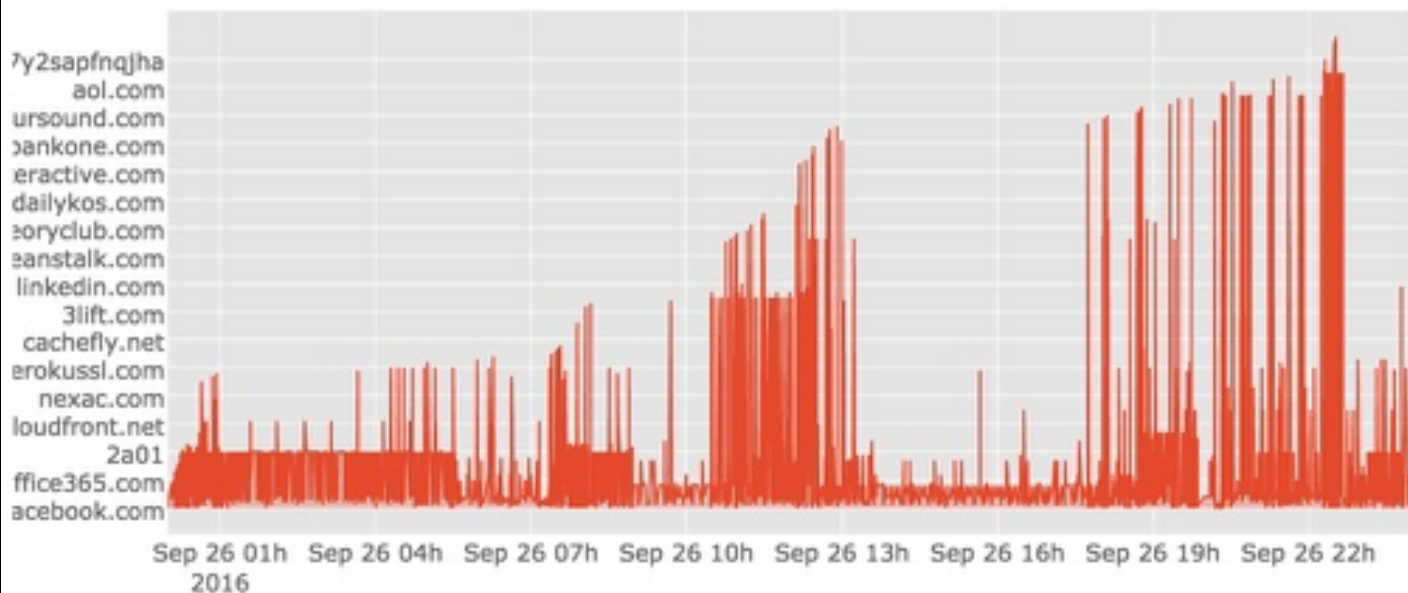
Sunday

Time Series from 09-25



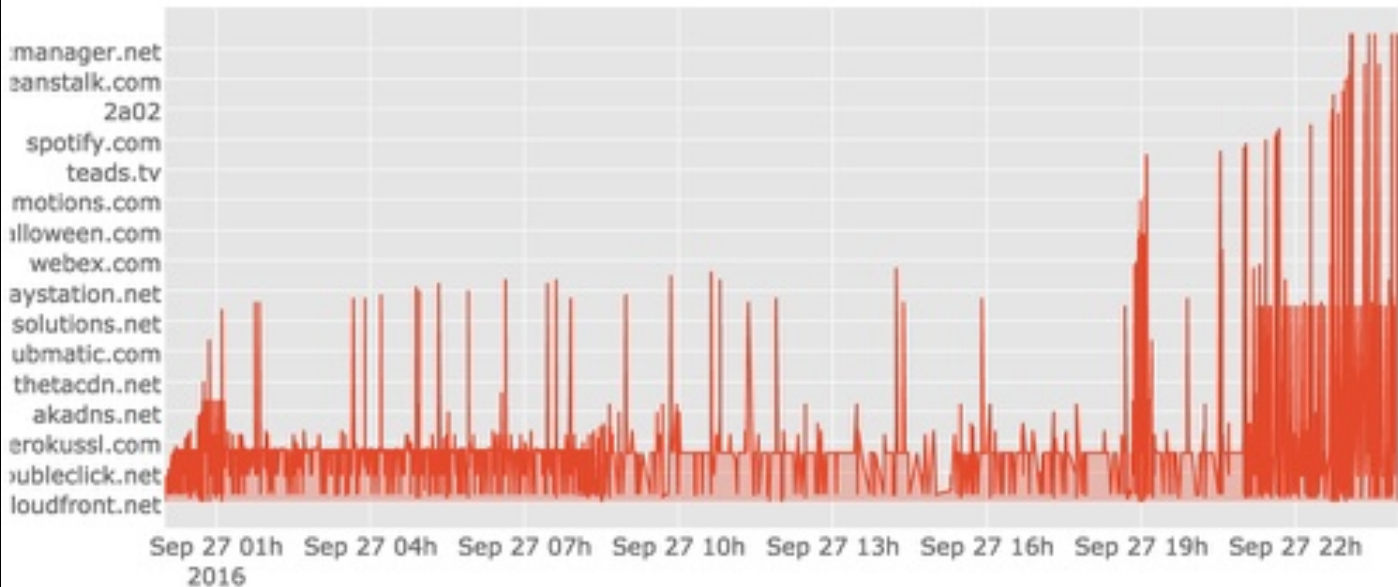
Monday

Time Series from 09-26



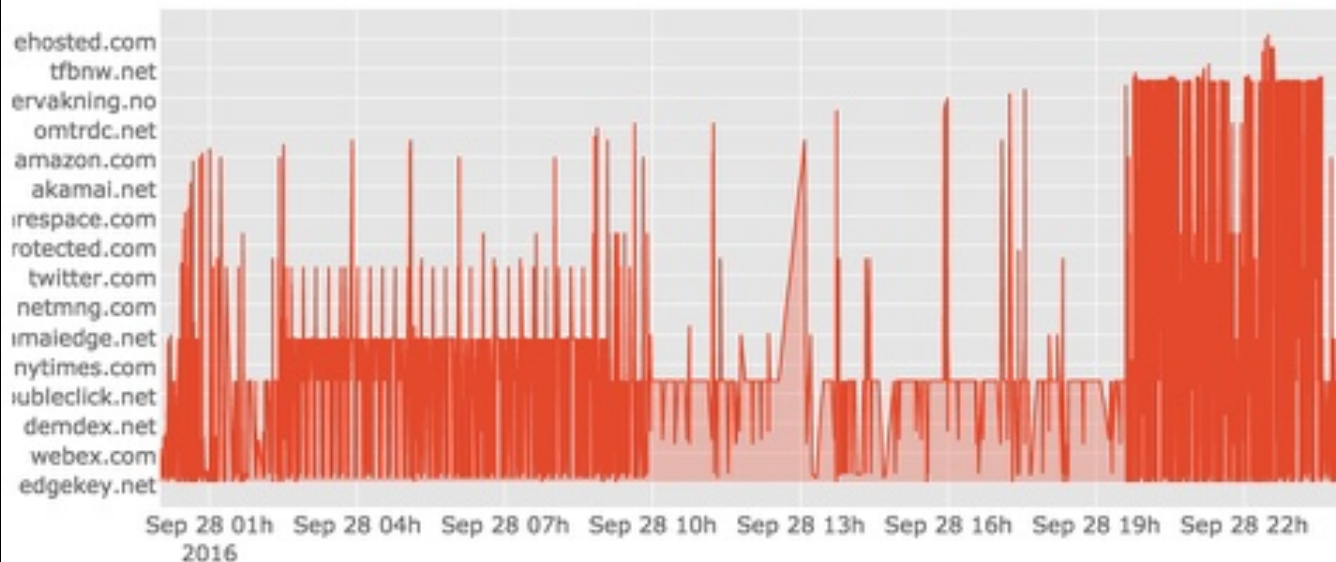
Tuesday

Time Series from 09-27



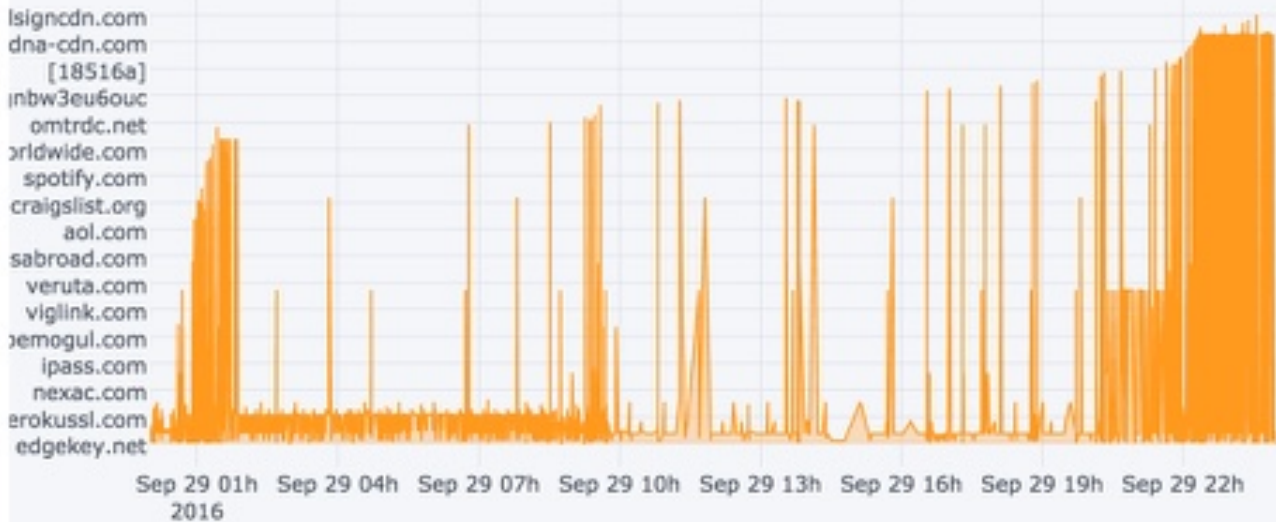
Wednesday

Time Series from 09-28



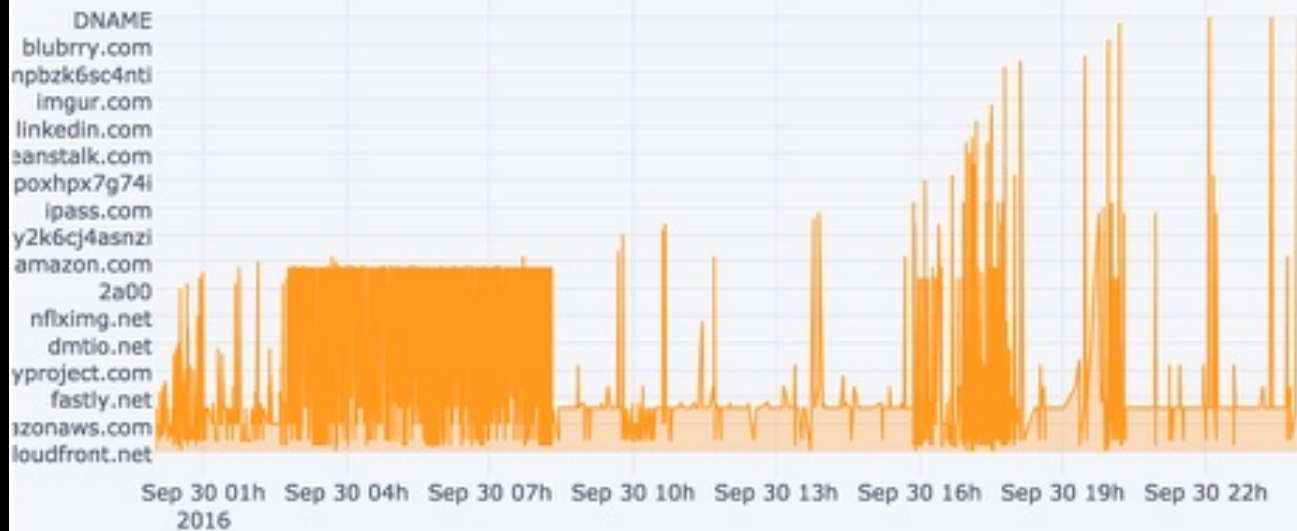
Thursday

Time Series from 09-29



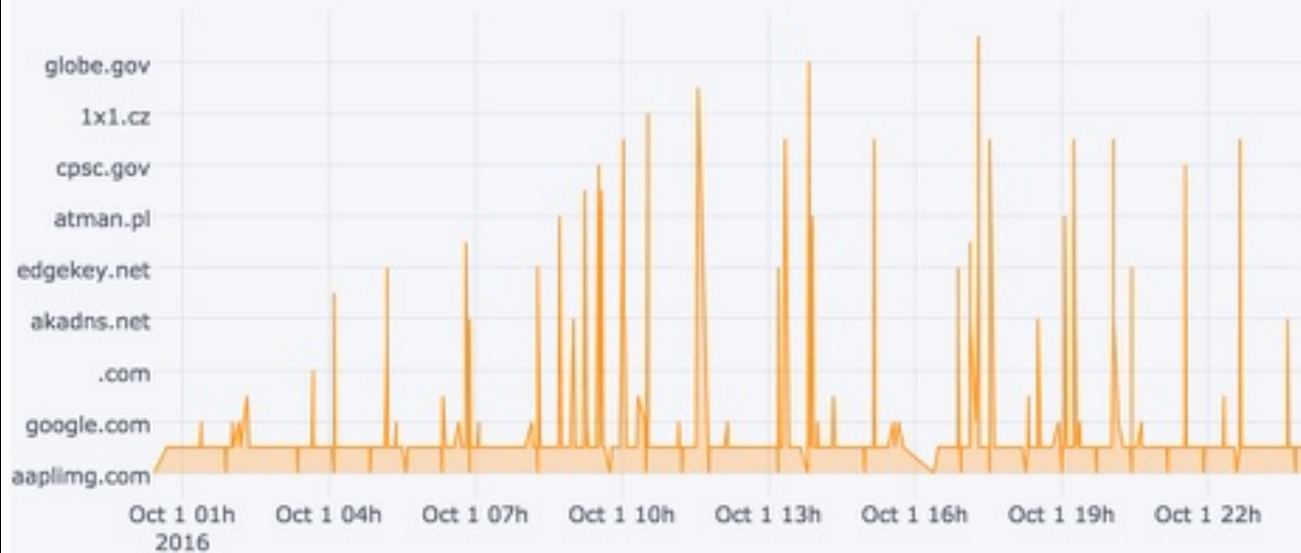
Friday

Time Series from 09-30



Saturday

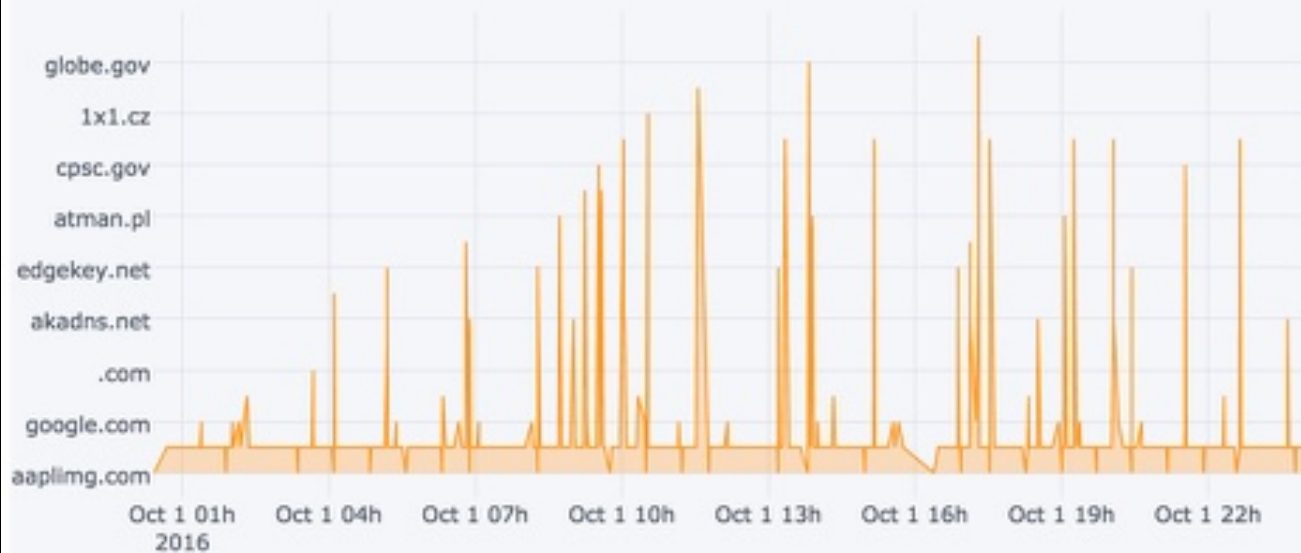
Time Series from 10-01



Not a lot of traffic

Saturday

Time Series from 10-01



Went out of town

Sunday

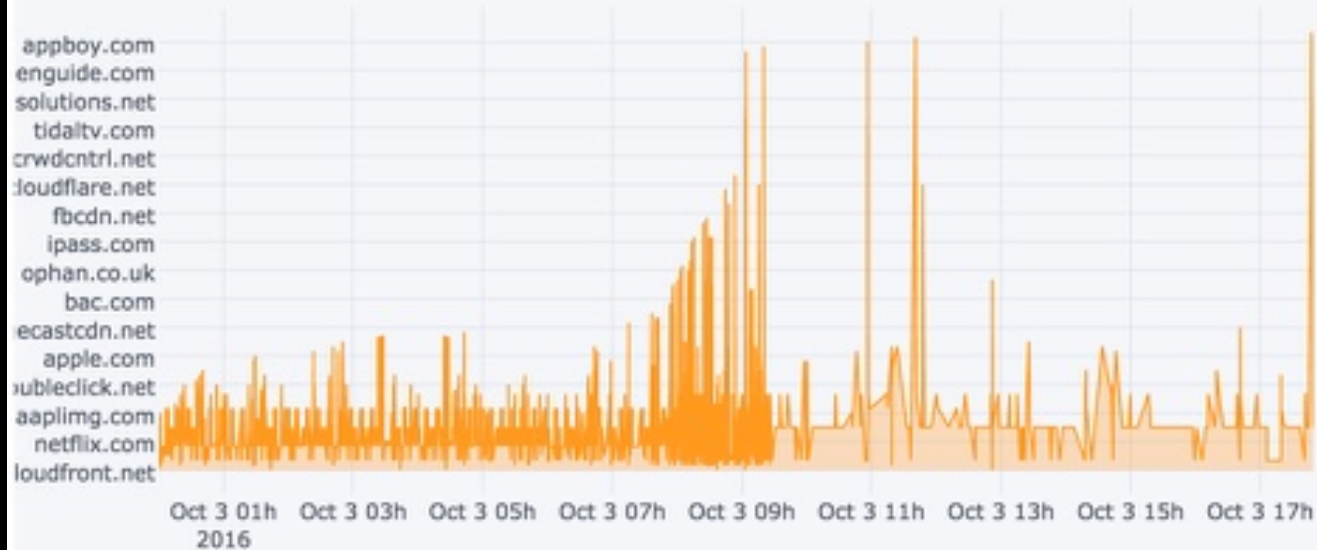
Time Series from 10-02

Still out of town ...and I'm home



Monday

Time Series from 10-03



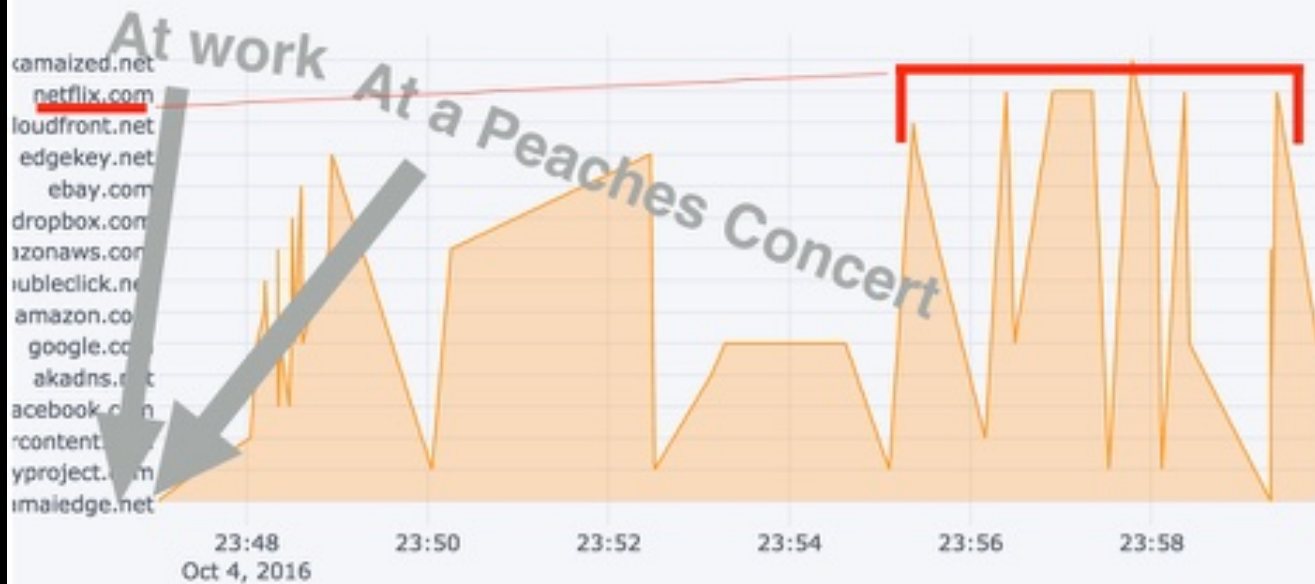
Tuesday

Time Series from 10-04

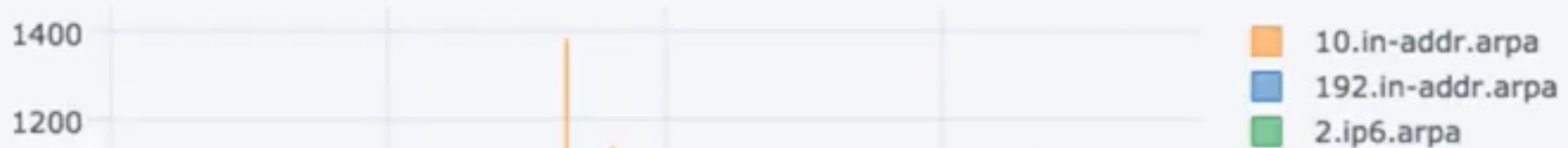


Tuesday

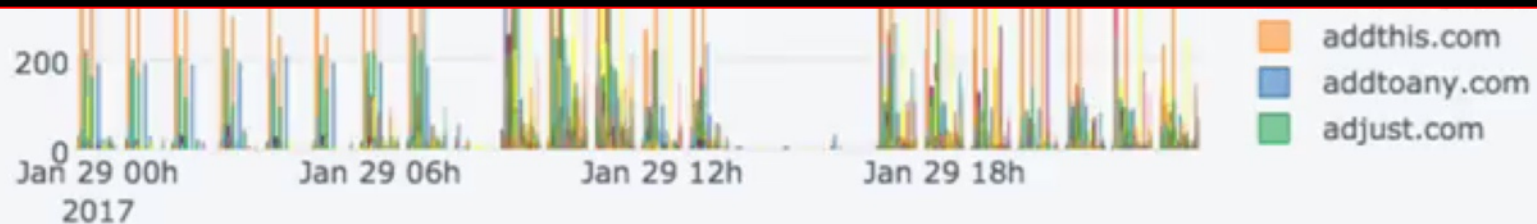
Time Series from 10-04



Time Series from Jan29



Video Showing when I
might be home based on activity



Save to a workable whatever

- Python -> MongoDB
- Influx DB -> Grafana
- LogStash -> ElasticSearch -> Kibana



Visualization

- Grafana
- Kibana
- Custom (Flask, D3, Plotly)



Grafana via InfluxDB (great for ongoing Timeseries)

Data Sources

+ Add data source



INFLUXDB



all_data default
http://localhost:8086

INFLUXDB



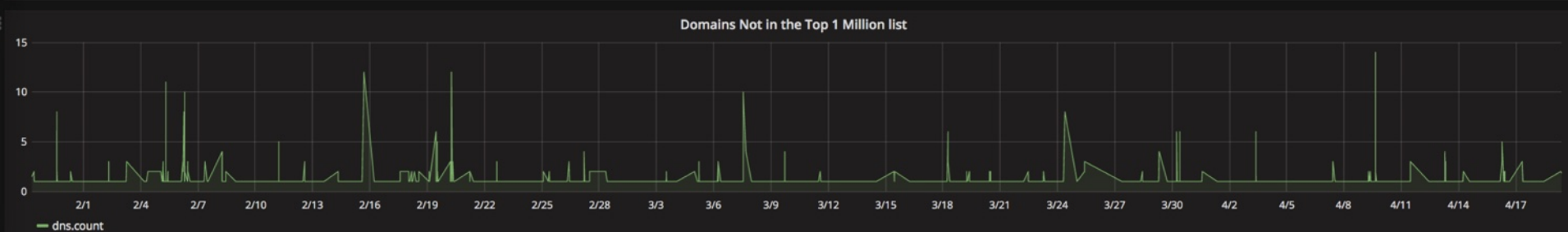
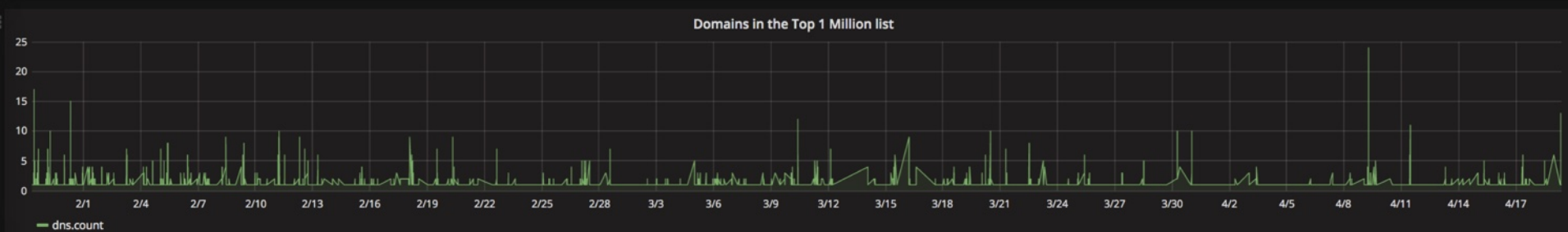
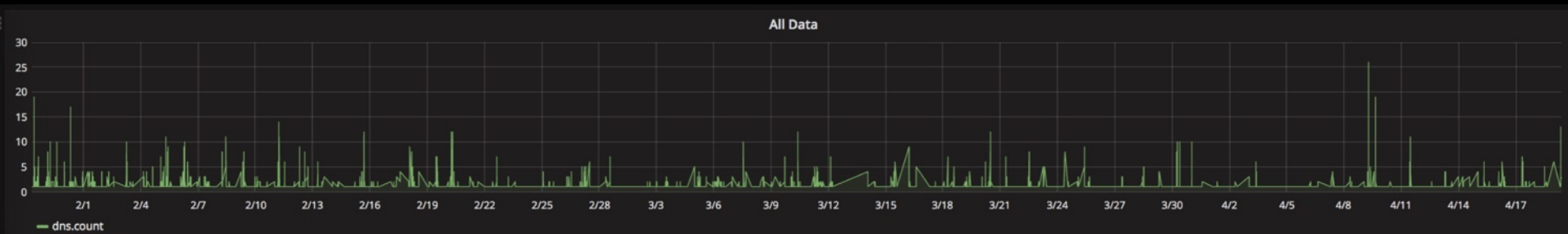
domains_in_to...
http://localhost:8080

INFLUXDB

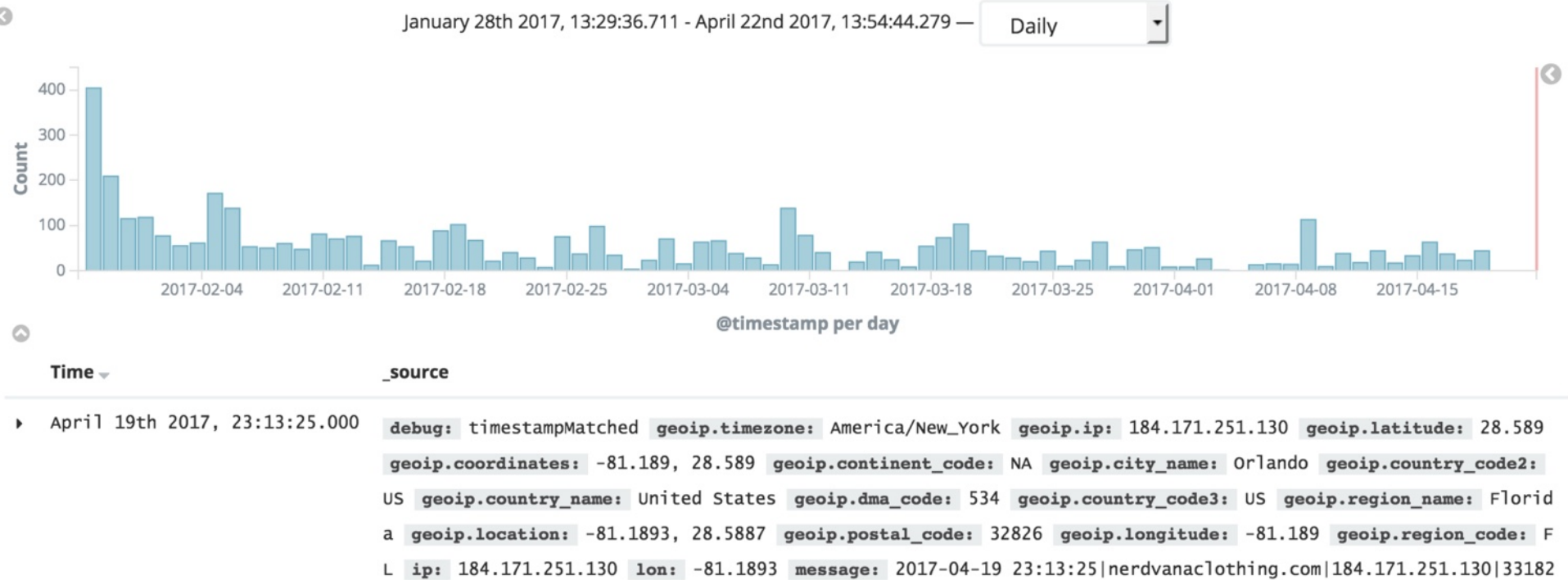


domains_not_i...
http://localhost:8080

Grafana via InfluxDB (great for ongoing Timeseries)



Kibana via Elasticsearch (ongoing Timeseries and more)



Filter...

Total Domains

2,857

Count

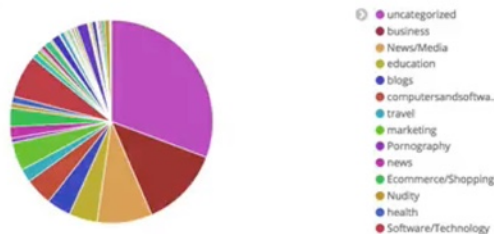
Map (all data)



Investigate Status (All)



Categories (all data)



Time Series (all data)

Domains in Top 1 Million List

2,201

Count

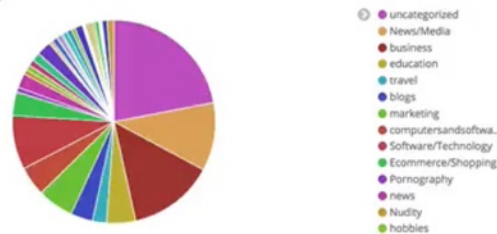
Map (domains in top 1 m)



Investigate Status (In Top 1 m)



Categories (in top 1 m)



Time Series (domains in top 1 m)

Domains not in top 1 Million List

656

Count

Map (domains not in top 1 m)



Investigate Status (Not in Top 1 m)



Categories (Not in top 1 m)

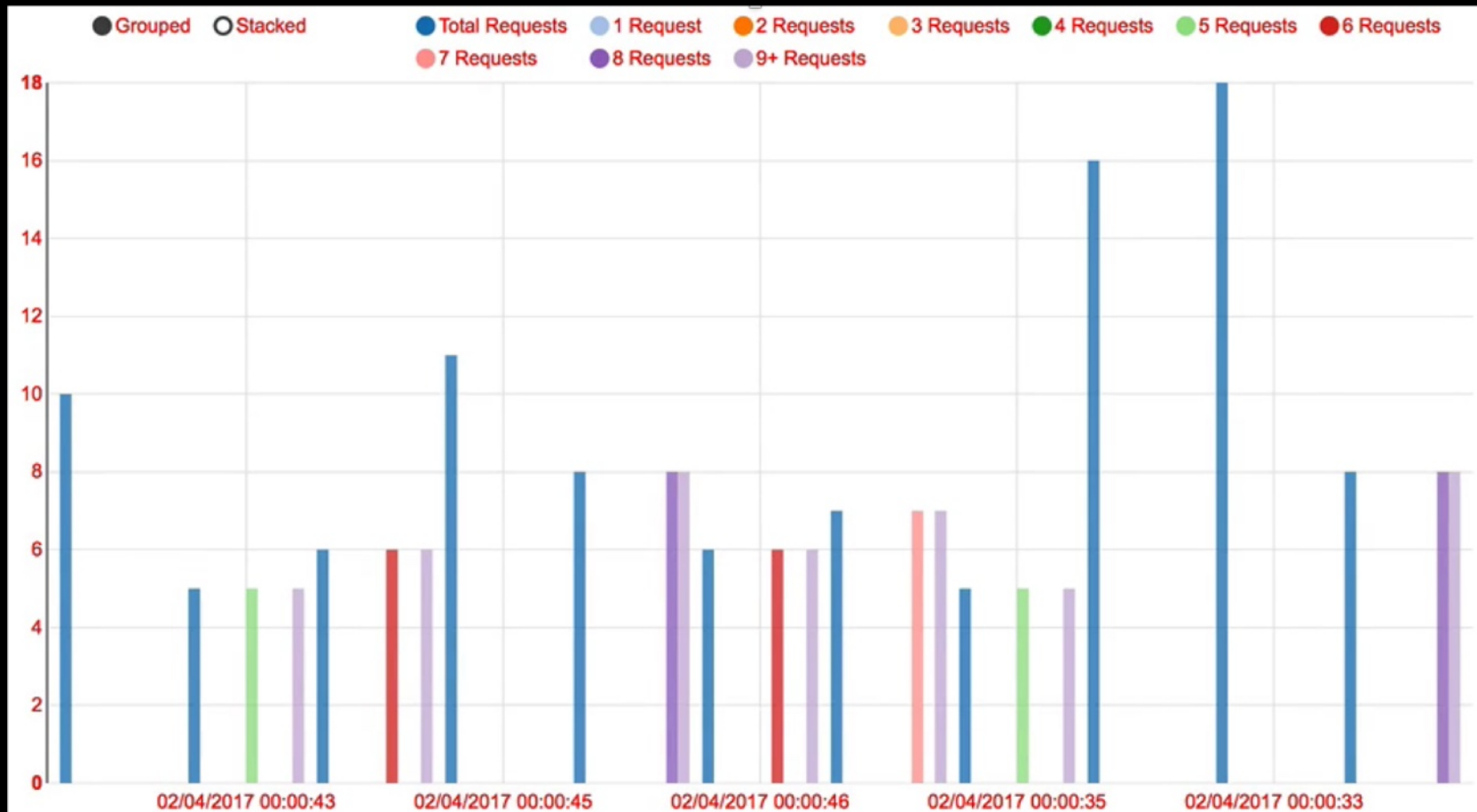


Time Series (domains not in top 1 m)

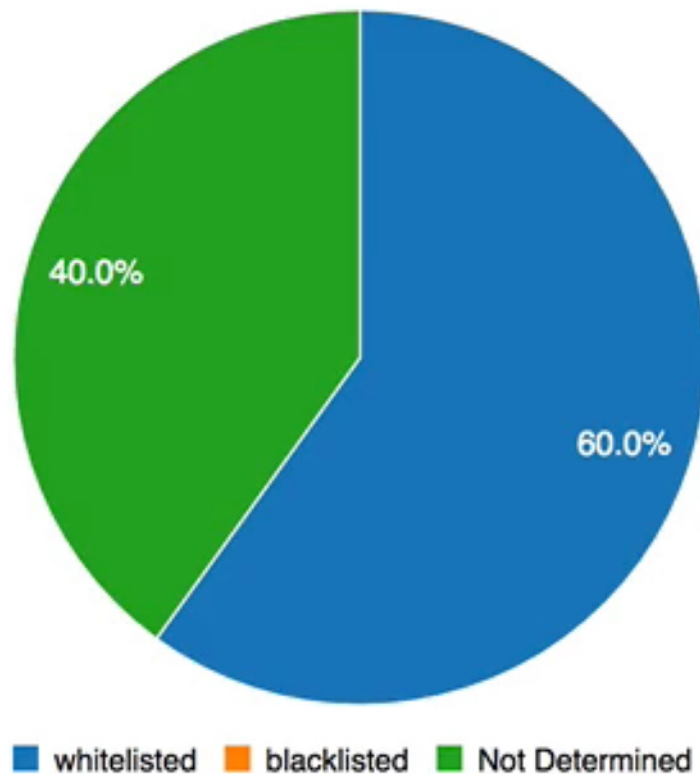
Visualization

- Grafana
- Kibana
- Custom (Flask, D3, Plotly)
 - Scripts auto-sending streaming data to MongoDB
 - Flask auto-processes from MongoDB
 - Flask serves content

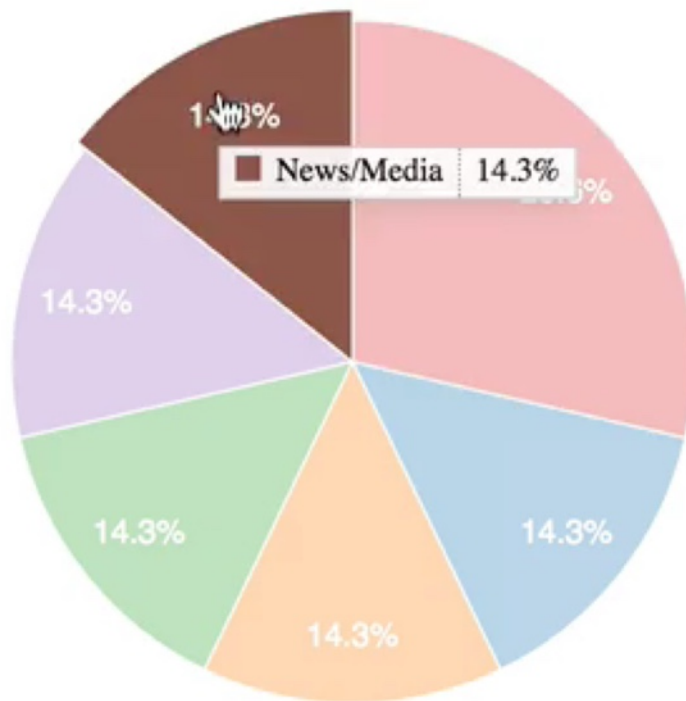




Investigate Security Categories



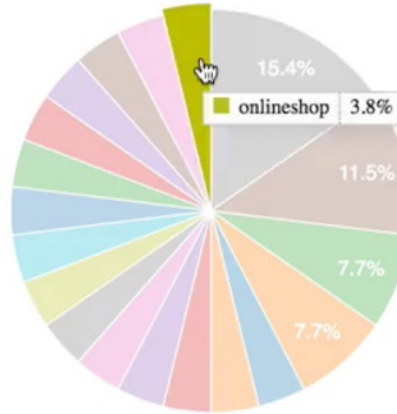
Investigate Categories



Blogs Podcasts Search Engines Radio Software/Technology News/Media



VirusTotal Categories



media file download shopping entertainment news and media marketing blogs streaming media social web - facebook radiomusic search engines and portals internet radio and tv
computers and software social networks business and economy search engines news education information technology onlineshop

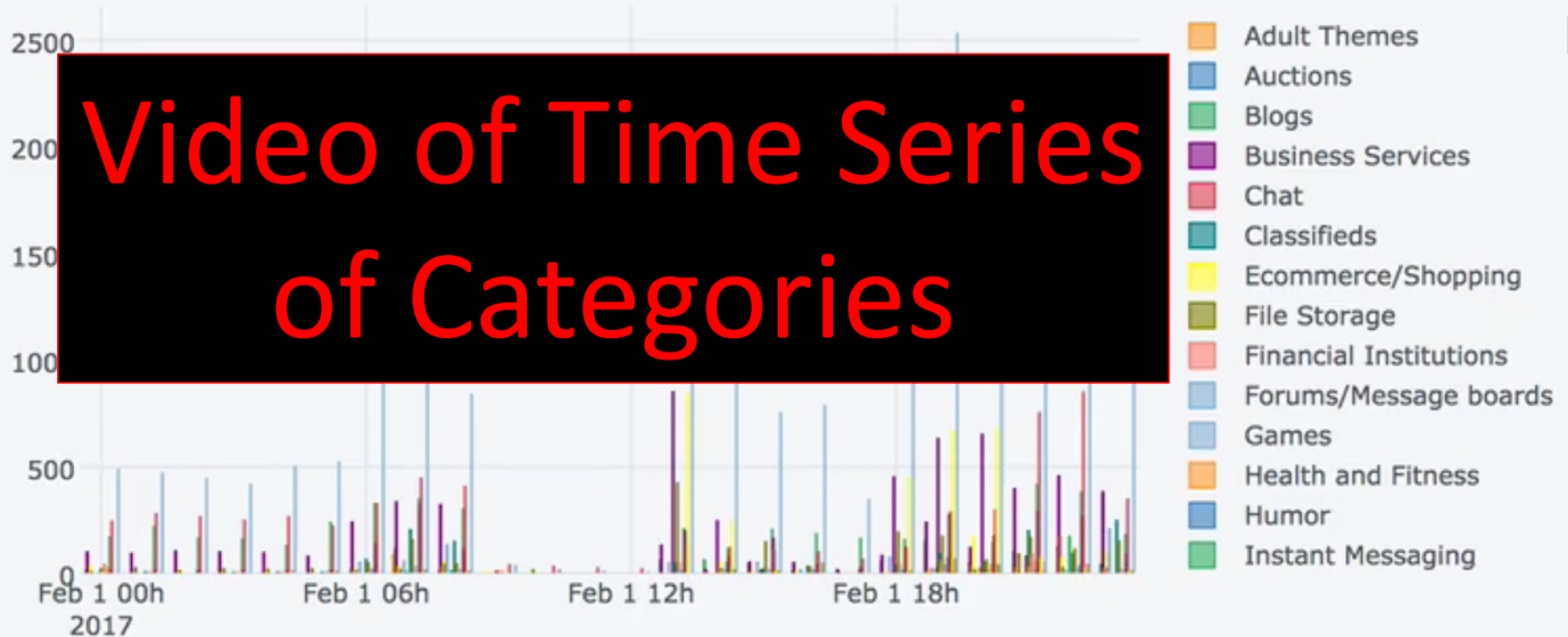


Categorization by Time

time	count	domain
2017-02-04 00:00:40	2	Search Engines
2017-02-04 00:00:46	6	Podcasts
2017-02-04 00:00:35	2	Search Engines
2017-02-04 00:00:44	8	Radio
2017-02-04 00:00:33	11	Search Engines
2017-02-04 00:00:43	2	Search Engines
2017-02-04 00:00:53	5	Blogs
2017-02-04 00:00:40	8	Software/Technology
2017-02-04 00:00:45	3	Radio
2017-02-04 00:00:53	5	News/Media
2017-02-04 00:00:45	2	Search Engines
2017-02-04 00:00:42	6	Podcasts
2017-02-04 00:00:53	5	Radio



Categories by Visit Time (Investigate)



Stats:

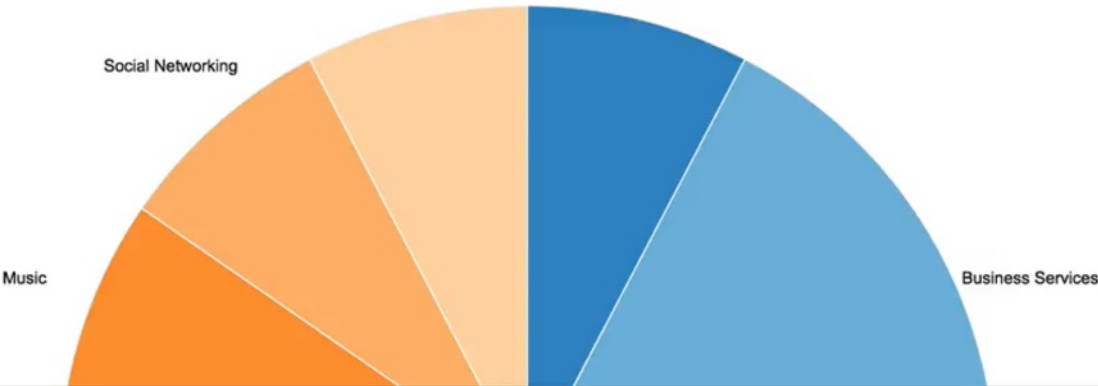
1083 unique domains seen
1183 total domains
100 total IP addresses
Normal traffic (domains visited over 3 times): 101
Amount of suspicious traffic domains visited under 2 times: 117

Of the suspicious domains (uniqued):
Whitelisted domains (OpenDNS): 8
Blacklisted domains (OpenDNS): 0
Neutral domains (OpenDNS): 2

Categories:

File Storage Business Services Software/Technology Search Engines Radio Music Social Networking Photo Sharing

Demo of DNS dashboard



All Traffic

View Map

Links open in a new tab: Domains, IP's, ASN, URLs open in Investigate, Samples in Threatgrid, Location in Google maps.

Time	Domain	IP	ASN	Location	Category	Reputation	Investigate Status	URLS
2017-01-29 00:00:12	life360.com	23.21.187.183	14618	Location	onlineshop	100,no,safe	0	
2017-01-29 00:00:37	songexploder.net	50.87.148.140	46606	Location	blogs	70,no,unsure	0	
2017-01-29 00:00:37	google.com	172.217.6.78	15169	Location	Search Engines	70,no,unsure	1	
2017-01-29 00:00:39	99percentinvisible.org	104.24.98.140	13335	Location	blogs	100,no,safe	0	http://99percentinvisible.org/wp-content/themes/ninety-nine/SCM/undefined/ , http://99percentinvisible.org/category/episode/ , http://99percentinvisible.org/ , http://99percentinvisible.org/
2017-01-29 00:00:44	feedburner.com	172.217.6.78	15169	Location	Software/Technology	100,no,safe	1	http://99percentinvisible.org/wp-content/themes/ninety-nine/SCM/undefined/ , http://99percentinvisible.org/category/episode/ , http://99percentinvisible.org/ , http://99percentinvisible.org/
2017-01-29 00:00:47	serialpodcast.org	104.20.17.241	13335	Location	marketing	70,no,unsure	0	http://serialpodcast.org/
2017-01-29 00:00:48	thisamericanlife.org	104.25.125.93	13335	Location	Radio	70,no,unsure	0	http://serialpodcast.org/
2017-01-29 00:00:49	theshawnstevensonmodel.com	162.144.255.131	20013	Location	education	100,no,safe	0	
2017-01-29 00:00:57	edgekey.net							
2017-01-29 00:00:13	amazonaws.com							downloads/311969/mkt.html/
2017-01-29 00:00:46	libsyn.com							invisible.org/">invisible.org/ , http://99percentinvisible.org/">http://99percentinvisible.org/
2017-01-29 00:00:57	blogtalkradio.com							
2017-01-29 00:00:57	akamaiedge.net							
2017-01-29 00:01:03	wnyc.org	52.204.43.74	14618	Location	News/Media	100,no,safe	0	
2017-01-29 00:01:27	google-analytics.com	172.217.6.68	15169	Location	computersandsoftware	100,no,safe	0	http://google-analytics.com/analytics-appset12 , http://google-analytics.com/
2017-01-29 00:01:28	cisco.com	72.163.4.161	109	Location	Software/Technology	100,no,safe	1	http://google-analytics.com/analytics-appset12 , http://google-analytics.com/
2017-01-29 00:02:12	crashlytics.com	54.225.129.210	14618	Location	Software/Technology	100,no,safe	0	http://google-analytics.com/analytics-appset12 , http://google-analytics.com/
2017-01-29 00:06:04	linksys.com	67.20.177.163	7381	Location	Software/Technology	100,no,safe	0	http://google-analytics.com/analytics-appset12 , http://google-analytics.com/
2017-01-29 00:06:37	73.in-addr.arpa	NO-IP	NO-ASN	Location	uncategorized		0	
2017-01-29 00:06:41	googleapis.com	172.217.6.68	15169	Location	computersandsoftware	100,no,safe	1	http://googleapis.com/gate.php http://googleapis.com/

Demo of Flask dashboard



Domains Not in Top 1 Million List

[View Map](#)

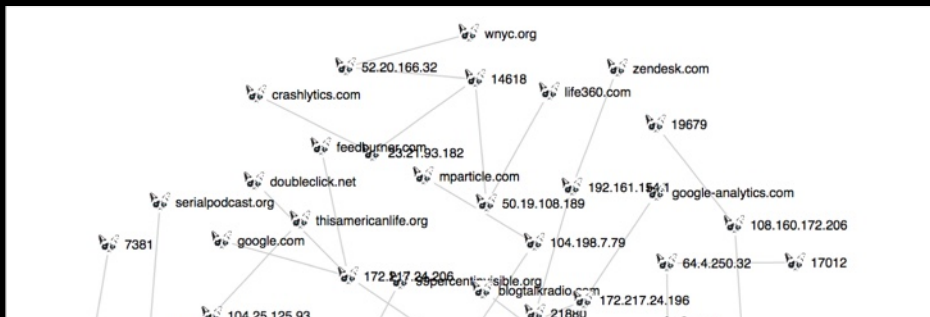
Links open in a new tab: Domains, IP's, ASN, URLS open in Investigate, Samples in Threatgrid, Location in Google maps.

Time	Domain	IP	ASN	Location	Investigate Status	Category
2017-01-29 00:00:49	theshawnstevensonmodel.com	162.144.255.131	20013	Location	0	education
2017-01-29 00:06:37	73.in-addr.arpa	NO-IP	NO-ASN	Location	0	uncategorized
2017-01-29 00:07:01	googleapis.com	172.217.6.68	15169	Location	1	computersandsoftware
2017-01-29 00:11:32	cloudfront.net	NO-IP	NO-ASN	Location	1	hosting
2017-01-29 00:31:50	evolt3.com	65.19.134.142	6939	Location	0	uncategorized
2017-01-29 00:47:09	gstatic.com	172.217.6.67	15169	Location	1	searchengines
2017-01-29 00:47:09	picanteberkeley.com	198.49.23.145	53831	Location	0	educational institutions
2017-01-29 07:20:25	appspot.com	172.217.6.81	15169	Location	1	Software/Technology
2017-01-29 07:20:37	fastlylb.net	NO-IP	NO-ASN	Location	1	information technology
2017-01-29 09:25:53	cloudapp.net	NO-IP	NO-ASN	Location	1	Software/Technology
2017-01-29 09:38:08	2.ip6.arpa	NO-IP	NO-ASN	Location	0	uncategorized
2017-01-29 09:54:18	n-theme.com	66.186.19.204	46844	Location	0	hosting
2017-01-29 10:25:49	plex.direct	82.94.168.7	3265	Location	0	business
2017-01-29 10:31:21	thecontrolleronline.com	103.13.240.67	33182	Location	0	games
2017-01-29 10:31:21	jeek.org	204.152.206.106	8100	Location	1	education
2017-01-29 10:31:22	hondashadow.net	75.126.50.202	36351	Location	0	hobbies
2017-01-29 12:00:48						
2017-01-29 12:05:50						
2017-01-29 12:07:41						
2017-01-29 12:09:49						
2017-01-29 12:20:16						
2017-01-29 12:33:33						
2017-01-29 13:01:55						
2017-01-29 17:59:12						
2017-01-29 17:59:12						
2017-01-29 18:07:47	usscpromotions.com	52.34.196.44	16509	Location	0	business
2017-01-29 18:07:52	tumblr.com	66.6.33.159	26101	Location	1	Blogs
2017-01-29 19:03:53	kravmaga-ikmf.com	191.233.85.165	8075	Location	0	sports
2017-01-29 19:09:18	ppehlab.org	198.49.23.144	53831	Location	0	uncategorized
2017-01-29 19:14:03	github.io	151.101.192.133	54113	Location	1	Blogs
2017-01-29 19:14:04	datarescuesfbay.org	192.30.252.153	36459	Location	0	uncategorized
2017-01-29 19:27:37	dnscsolution.com	162.253.104.105	20141	Location	0	business
2017-01-29 20:29:10	bsidessf.com	104.24.99.203	13335	Location	0	information technology
2017-01-29 23:01:30	usuncut.news	NO-IP	NO-ASN	Location	0	uncategorized
2017-01-29 23:18:16	deusex.com	34.198.79.90	14618	Location	0	Games
2017-01-29 23:34:06	azurewebsites.net	NO-IP	NO-ASN	Location	1	Software/Technology
2017-01-30 09:18:11	67.in-addr.arpa	NO-IP	NO-ASN	Location	0	uncategorized
2017-01-30 09:42:32	envirodatagov.org	104.219.248.97	22612	Location	0	uncategorized

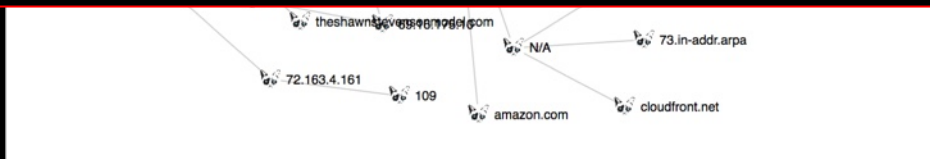
Demo of Flask dashboard



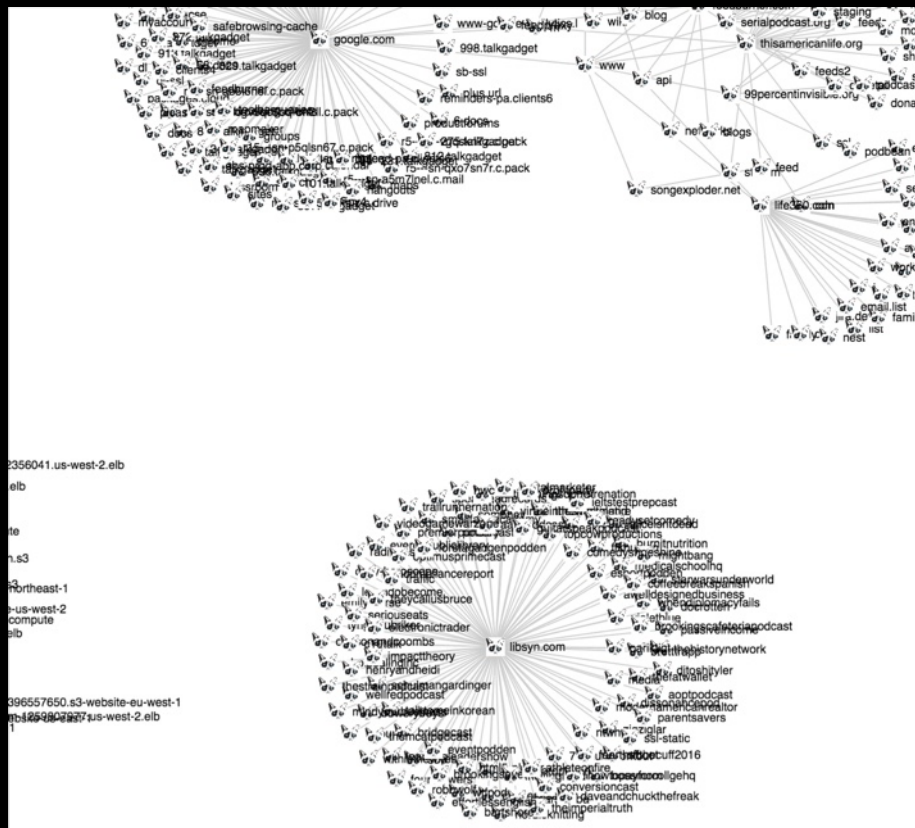
Category Mapping



Demo of Additional
Visualization tools



Subdomain Mapping



Just Mapping



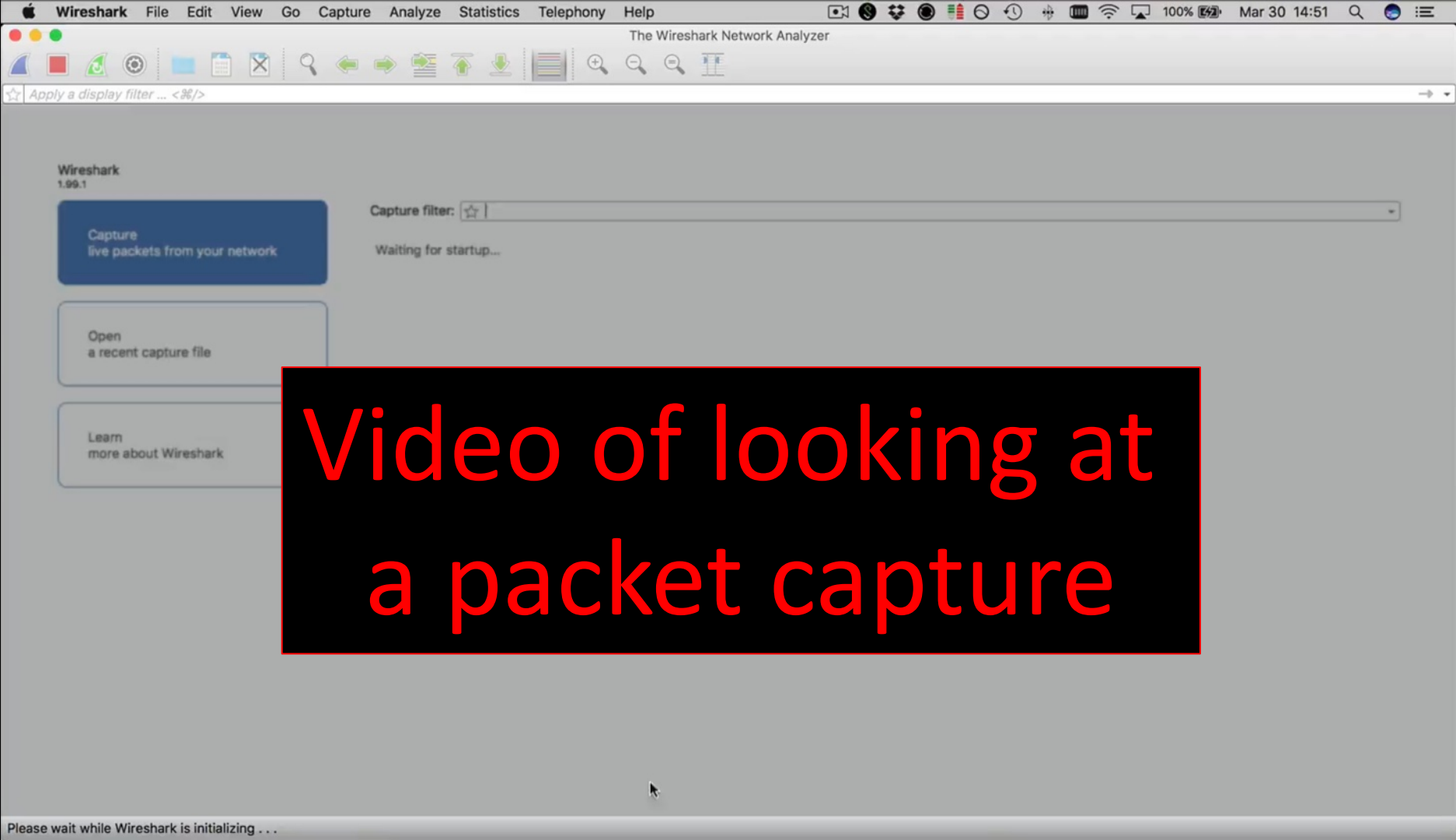
BEHAVIORAL ANALYSIS USING DNS & NETWORK TRAFFIC



Network Traffic / Captures

- DPKT Python Packet Library
- Grab all the HTTP traffic
- Generate Statistics





Stats:

255 GET requests seen
2 POSTS seen
3 total Source IP addresses
25 total Destination IP addresses
32 total Destination Hosts

GETs vs POSTs:

● GET Requests ● POSTs

Packet capture visualization dashboard

riangularllc.com, 107.182.162.228, GET

26-09-2016 10:38:11:374819, 172.16.212.140, triangularllc.com, 107.182.162.228, GET

26-09-2016 10:38:11:374985, 172.16.212.140, triangularllc.com, 107.182.162.228, GET

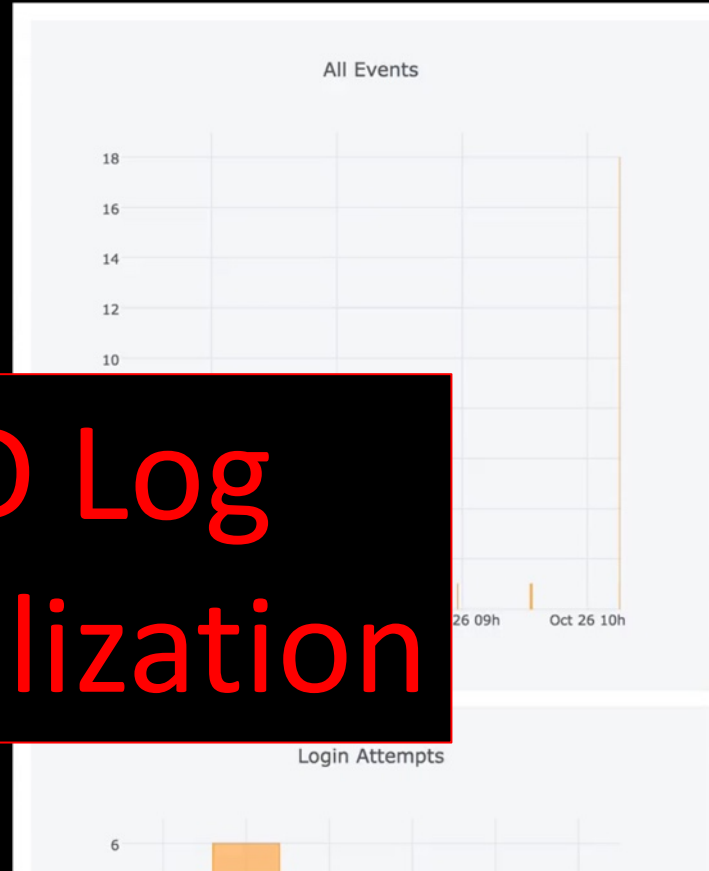
26-09-2016 10:38:11:375729, 172.16.212.140, triangularllc.com, 107.182.162.228, GET

Timeline:

Active Directory Logs

- Successful VS Failed Logins

AD Log
visualization



Does it run? Just leave it alone.



Writing Code that Nobody Else Can Read

The Definitive Guide

ations Slide Show Review View

100 A A

U obe X² X₂ A₂ A

Convert to SmartArt Picture Shapes Text Box Arr

app

> Search

Name	Date Modified	Size	Kind
10.txt	Yesterday, 4:58 PM	764 bytes	Plain Text
100.txt	Yesterday, 3:03 PM	8 KB	Plain Text
1000.txt	Mar 28, 2017, 10:36 PM	83 KB	Plain Text
build	Mar 24, 2017, 4:49 PM	--	Folder
config	Mar 24, 2017, 10:16 AM	--	Folder
domaintoasn	Mar 24, 2017, 2:55 PM	--	Folder
Feb1.txt	Mar 28, 2017, 2:53 PM	3.8 MB	Plain Text
Feb2.txt	Mar 28, 2017, 2:53 PM	2.5 MB	Plain Text
Feb3.txt	Mar 28, 2017, 2:53 PM	3 MB	Plain Text
Feb4.txt	Mar 28, 2017, 2:53 PM	4.4 MB	Plain Text
Feb5.txt	Mar 28, 2017, 2:53 PM	6.2 MB	Plain Text
investigate	Mar 24, 2017, 3:44 PM	--	Folder
invest.py	Today, 12:21 PM	9 KB	Python
process_tcpdump_by_day.py	Mar 28, 2017, 5:49 PM	8 KB	Python
stream.py	Mar 12, 2017, 12:50 AM	3 KB	Python
tester.py	Today, 11:53 AM	33 KB	Python
timeseries	Today, 12:21 PM	--	Folder
c3_timeseries.html	Mar 24, 2017, 4:31 PM	3 KB	HTML doc
dataframe.html	Today, 12:21 PM	18 KB	HTML doc
feb1_categories.html	Yesterday, 10:38 PM	24 KB	HTML doc
Feb2_ts.html	Today, 12:21 PM	27 KB	HTML doc
linechart.html	Mar 19, 2017, 2:29 PM	1 KB	HTML doc
nvd3_time_series.json	Mar 21, 2017, 3:28 PM	3 KB	JSON
nvd3_timeseries.html	Mar 21, 2017, 4:19 PM	5 KB	HTML doc
pie.html	Mar 16, 2017, 2:56 PM	6 KB	HTML doc
plotly_category_ts.html	Yesterday, 2:26 PM	2 KB	HTML doc
plotly_timeseries.html	Mar 21, 2017, 4:19 PM	4 KB	HTML doc
test.html	Mar 27, 2017, 12:27 AM	1 KB	HTML doc
ts_counts.html	Yesterday, 11:30 AM	4 KB	HTML doc
to do.txt	Mar 21, 2017, 4:13 PM	313 bytes	Plain Text
virustotal	Mar 24, 2017, 3:48 PM	--	Folder

1 of 31 selected, 59.55 GB available

Some Considerations...



Not Yet a Perfect Solution

- Intrusion Detection, AV and User awareness still have their place
- Analyzing Behavior can decrease the amount of work you have to do
- Can provide more visibility
- Potential to alert you about anomalies before anything else



If you don't want to be watched

- Use a VPN on each device or on your network
- Use your own DNS Server (and send it through that VPN)
- You can learn a lot about who you're watching






**INTELLIGENT
DEFENCE**

infosecurity[®]
EUROPE



GitHub, Inc. [US] <https://github.com/jpyorre>

Search GitHub Pull requests Issues Gist



Josh Pyorre
jpyorre

[Add a bio](#)

📍 Oakland, CA
🕒 Joined on Jan 11, 2013

<https://jpyorre.com>
jpyorre@gmail.com
@cisco.com
@opendns.com

Overview Repositories 4 Stars 0 Followers 10 Following 0

Popular repositories

IntelligentHoneyNet
The Intelligent Honey Net Project attempts to create actionable information from honeypots
Python ★ 25 🍴 7

cut-copy
Scripts for randomizing text and audio data (To work with lyrics and audio files)
Python

datasharing
Forked from [jtleek/datasharing](#)
The Leek group guide to data sharing

behavioral_analysis
Jupyter Notebook

 **@joshpyorre**