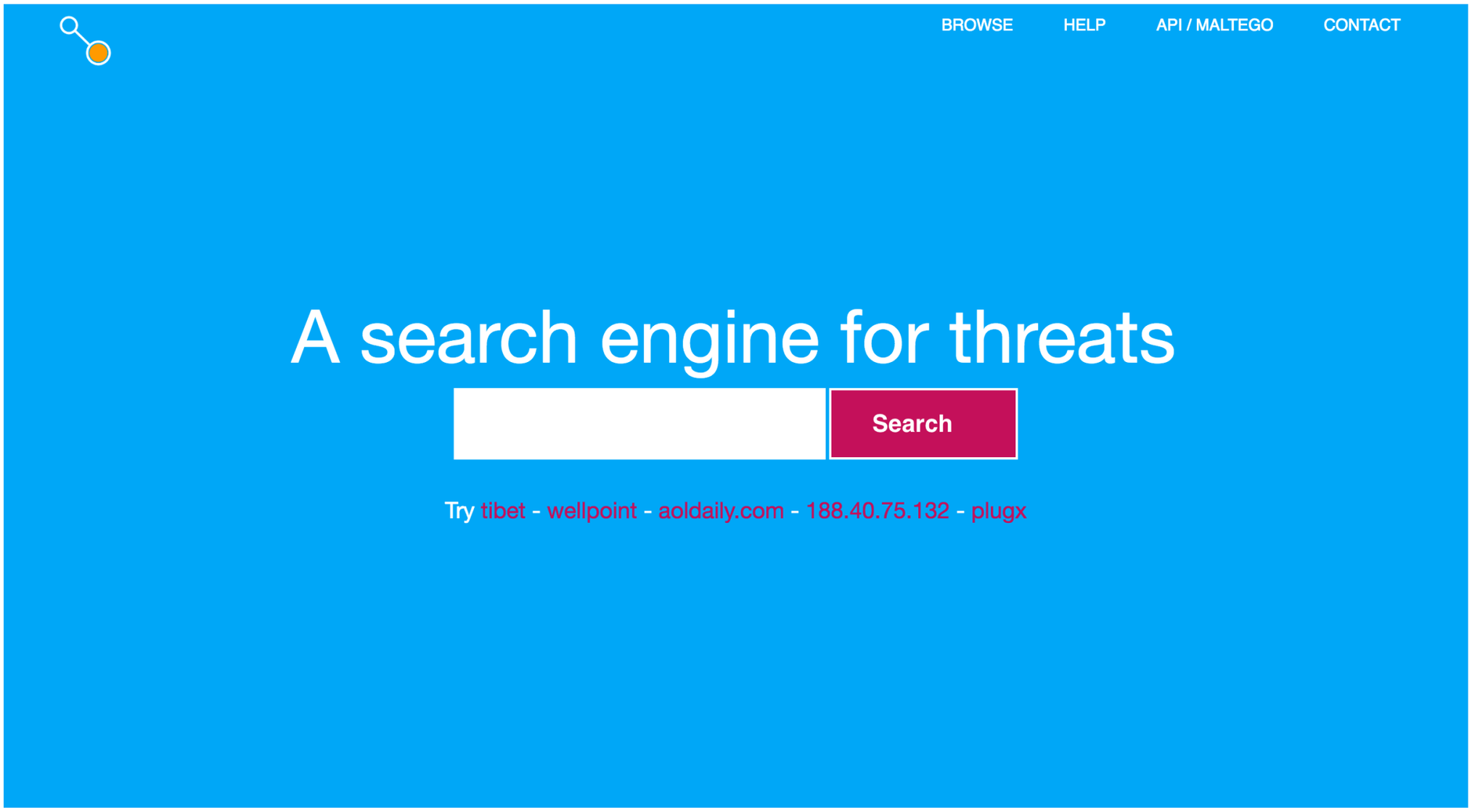
ThreatCrowd.org

@chrisdoman, VECTRA

bsidesbelfast.org September 2016

What is ThreatCrowd?

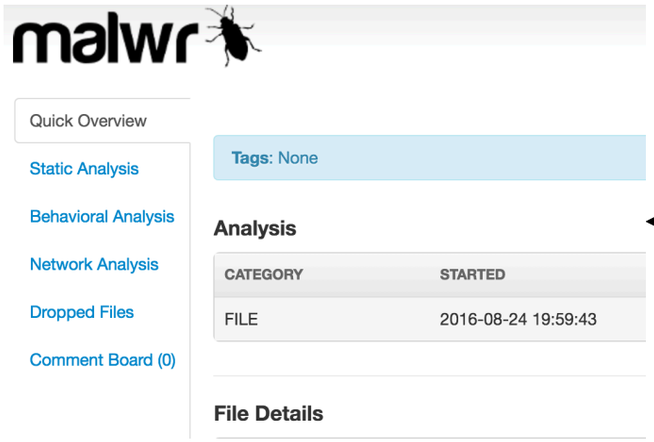


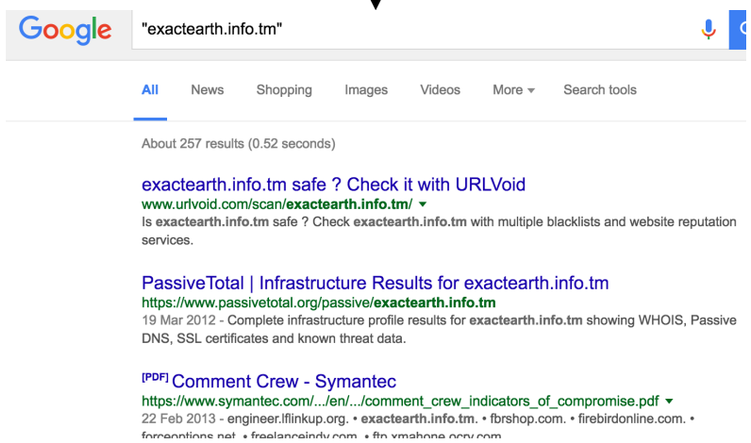
threatcrowd.org

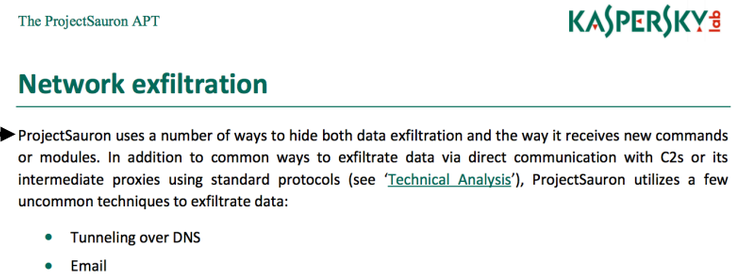
Use-case: ThreatIntel & Triaging Detections

baddomain.com

Source IP	Destination IP	Event Signature
178.238.86.19	192.168.1.108	sensitive_data: sensitive data global threshold excee...
178.238.86.19	192.168.1.108	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENC...
208.80.52.156	67.172.135.80	http_inspect: NO CONTENT-LENGTH OR TRANSFER-ENC...







Use Case: Bug-Bounties & Pen-Tests

Search

Search by Domain,IP,Email or Organisation

SE HELP API FEED MALTEGO CONTA

tibet.zyns.com
Reference=https://raw.githubusercontent.com/citizenlab/malware-indicators/master/network-indicators.csv MD5=098fd5532587f7391c7f20e4e16af13d MD5=7F7CBC62C56AEC9CB351B6C1B1926265

tibet.my03.com
Reference=https://raw.githubusercontent.com/citizenlab/malware-indicators/master/network-indicators.csv MD5=6c1fa0a523a751b8d588b75814a46759

tibet.mercifulland.com
Reference=http://www.tcrc.edu.tw/cert/20111215.xlsx

tibetcongress.oicp.net
Reference=https://otx.alienvault.com/pulse/56a770e167db8c6aaee00fa5/ Reference=https://www.virustotal.com/en/ip-address/174.128.255.230/information/

tibetantimes.ezua.com
Reference=http://targetedthreats.net/media/2.2%20Extended%20Analysis-Cluster.pdf Reference=https://raw.githubusercontent.com/citizenlab/malware-indicators/master/network-indicators.csv

tibet.cpc.people.com.cn

tibet.people.com.cn

tibet-zj.vicp.cc

tibet.freeserve.co.uk

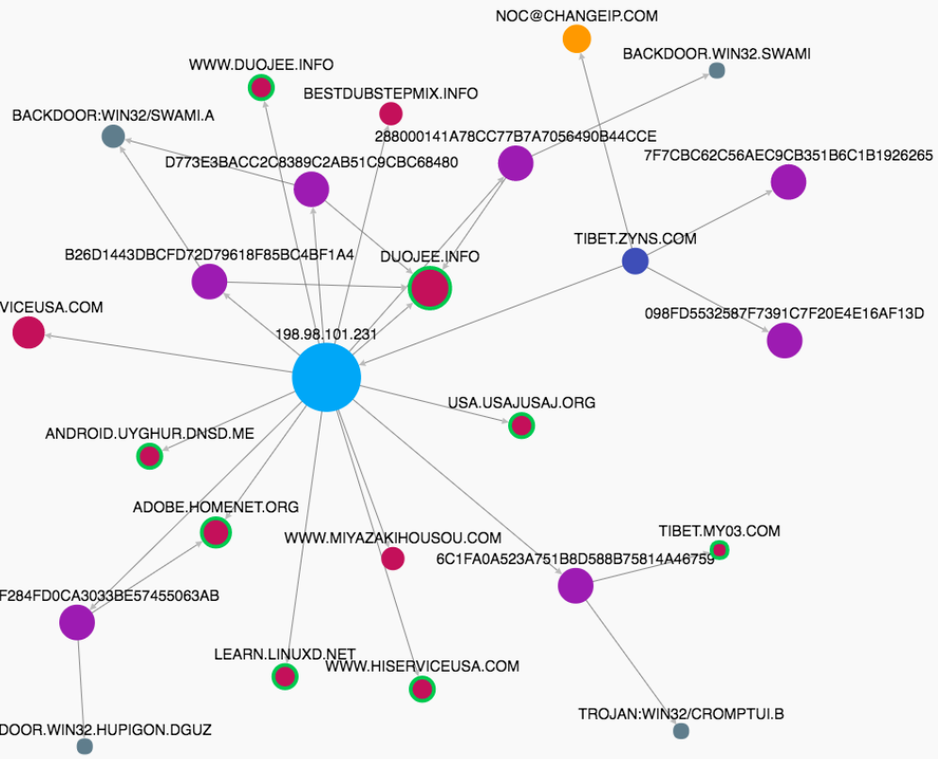
tibet-barma.tibet-barma.cz

tibetannews.office-sevice.com
Reference=https://raw.githubusercontent.com/citizenlab/malware-indicators/master/network-indicators.csv

Infrastructure

Search by Domain,IP,Email or Organisation

HELP RSS API FEED MALTEGO CONTACT @CHRIS DOMAN



DOMAIN > TIBET.ZYNS.COM

Most users have voted this as MALICIOUS

Is this malicious? Yes No

RESULTS

https://raw.githubusercontent.com/citizenlab/malwa...

FILES THAT TALK TO TIBET.ZYNS.COM

MD5	A/V
7F7CBC62C56AEC9CB351B6C1B1926265	
098fd5532587f7391c7f20e4e16af13d	

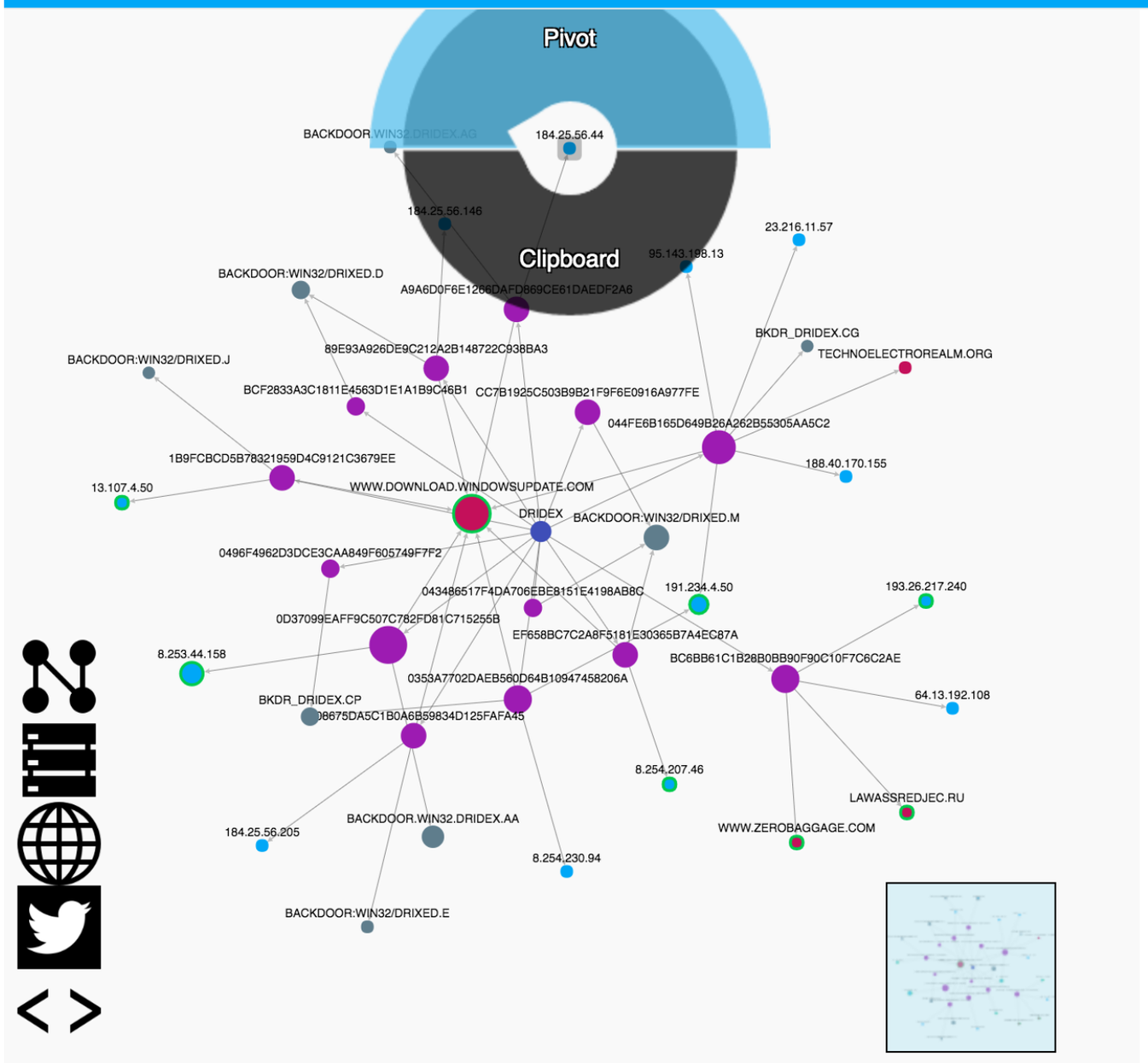
WHOIS DETAILS

Property	Value
Name	Network OperationsZZZ, ChangeIP (78)
Email	noc@changeip.com (546)
Address	1200 Brickell Avenue
Zip Code	33131

Pivot

Search by Domain,IP,Email or Organisation

HELP RSS API FEED MALTEGO CONTACT @CHRIS DOMAN



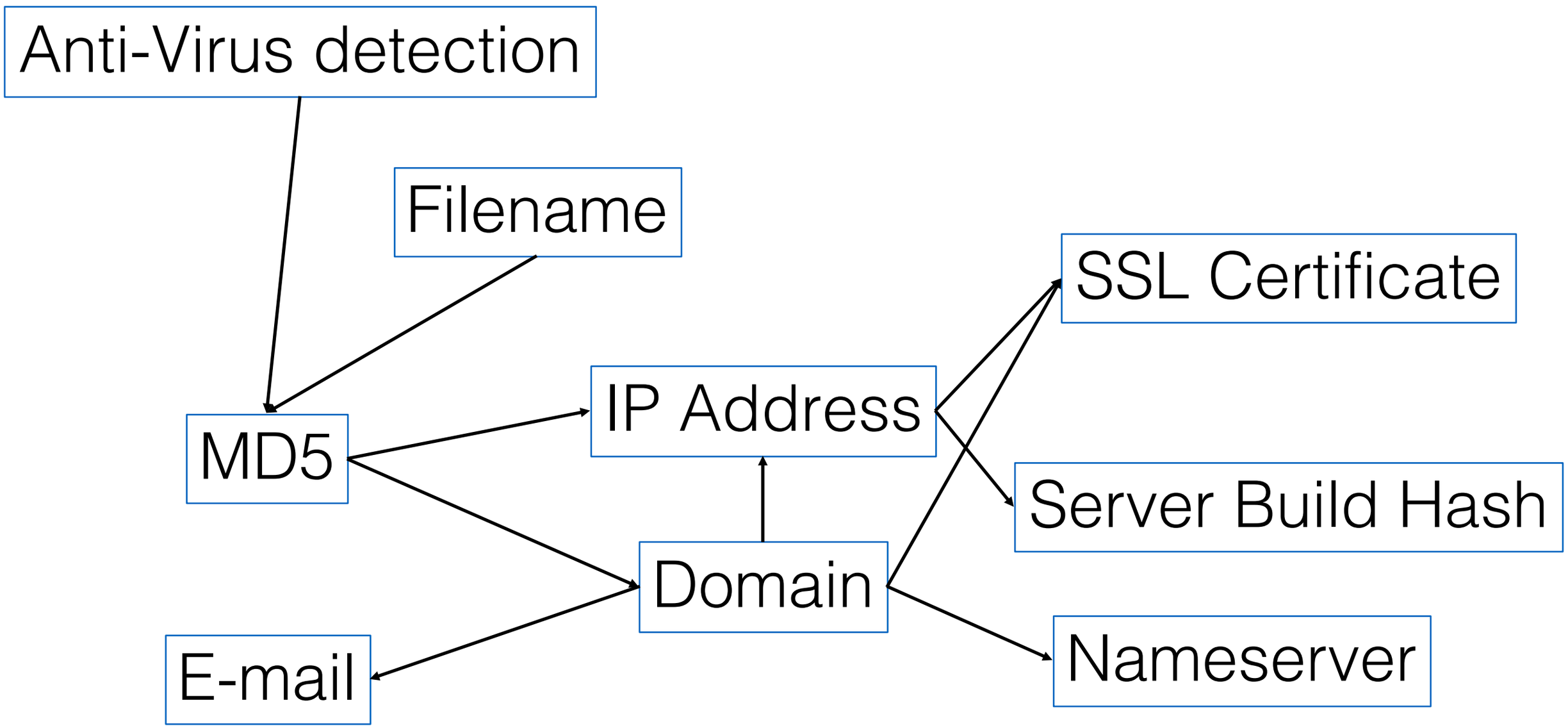
MALWARE > DRIDEX

1-100 of 849 results.

[Next]

MD5	Domains
0d37099eaff9c507c782fd81c715255b	[www.download.windowsupdat...]
a9a6d0f6e1266dafd869ce61daedf2a6	[www.download.windowsupdat...]
cc7b1925c503b9b21f9f6e0916a977fe	
bc6bb61c1b28b0bb90f90c10f7c6c2ae	[lawassredjec.ru] [www.zerobaggage.com]
0d37099eaff9c507c782fd81c715255b	[www.download.windowsupdat...]
cc7b1925c503b9b21f9f6e0916a977fe	
ef658bc7c2a8f5181e30365b7a4ec87a	[www.download.windowsupdat...]
1b9fcbcd5b78321959d4c9121c3679ee	[www.download.windowsupdat...]
044fe6b165d649b26a262b55305aa5c2	[technoelectrorealm.org] [www.download.windowsupdat...]
89e93a926de9c212a2b148722c938ba3	[www.download.windowsupdat...]
bcf2833a3c1811e4563d1e1a1b9c46b1	
0353a7702daeb560d64b10947458206a	[www.download.windowsupdat...]

Pivot



Automatically identify sinkholes and parking ranges, and avoid pivoting

Browse

BROWSE

The following malware reports are automatically extracted and presented within ThreatCrowd.

http://0xicf.wordpress.com/2014/12/18/a-pirated-version-of-the-assassins-creed-application-for-android-is-bundled-with-malware/
http://2014.zeronights.ru/assets/files/slides/roaming_tiger_zeronights_2014.pdf
http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/2q-report-on-targeted-attack-campaigns.pdf
http://androguard.blogspot.com/2011/06/droidbox-testing-with-geinimi-sample.html
http://arstechnica.com/security/2012/08/gauss-espionage-malware-phones-home-to-same-servers-as-iran-targeting-flame/
http://badoo.com/install/?ref=new_design_email
http://bartblaze.blogspot.com/2014/11/malware-spreading-via-steam-chat.html
http://bartblaze.blogspot.com/2015/02/yet-another-ransomware-variant.html
http://bartblaze.blogspot.com/2015/09/notes-on-linuxxorddos.html
http://bartblaze.blogspot.com/2015/11/a-quick-look-at-signed-spam-campaign.html
http://bartblaze.blogspot.com/2015/11/more-ransomware-shenanigans.html
http://bartblaze.blogspot.com/2016/02/vipasana-ransomware-new-ransom-on-block.html
http://bit.ly/1BFEujv
http://blog.0day.jp/2015/06/linuxmayhem.html
http://blog.0x3a.com/post/110052845124/an-in-depth-analysis-of-the-fiesta-exploit-kit-an
http://blog.0x3a.com/post/114659871819
http://blog.0x3a.com/post/120423677154/unusual-njrat-campaign-originating-from-saudi
http://blog.0x3a.com/post/126900680679/analysis-of-a-piece-of-ransomware-in-development

Blacklists

Crowdsourcing America's cybersecurity is an idea so crazy it might just work

https://www.threatcrowd.org/feeds/domains.txt

```
0906.toh.info
0n4tblbdfncaauxioxto.ddns.net
0xota.com
1000homemovis.com
1001010.org
10yearsofborn.com
11111111.noip.me
111xxx.com
112038398dc590fd910f04439eba2dc2.ovh
11vbvb.com
12-68.xicp.net
14mdbbx3242lm5q.net
16qvklkb3b58sfix54kf5lq.ddns.net
1845realty.com
18andabused.com
1nsmm.bpa.nu
1qw2.wha.la
1rot1ro05p5pc654ktuj74i.ddns.net
1rx.io
1uer3u9vttynxg.com
1vp412e12nheix.net
1vyrexifwt5rqpwvepm.ddns.net
1x1te0o878iponovyja8m87.ddns.net
```

DOMAIN > TIBET.MY03.COM

Most users have voted this as MALICIOUS

Is this malicious? Yes No

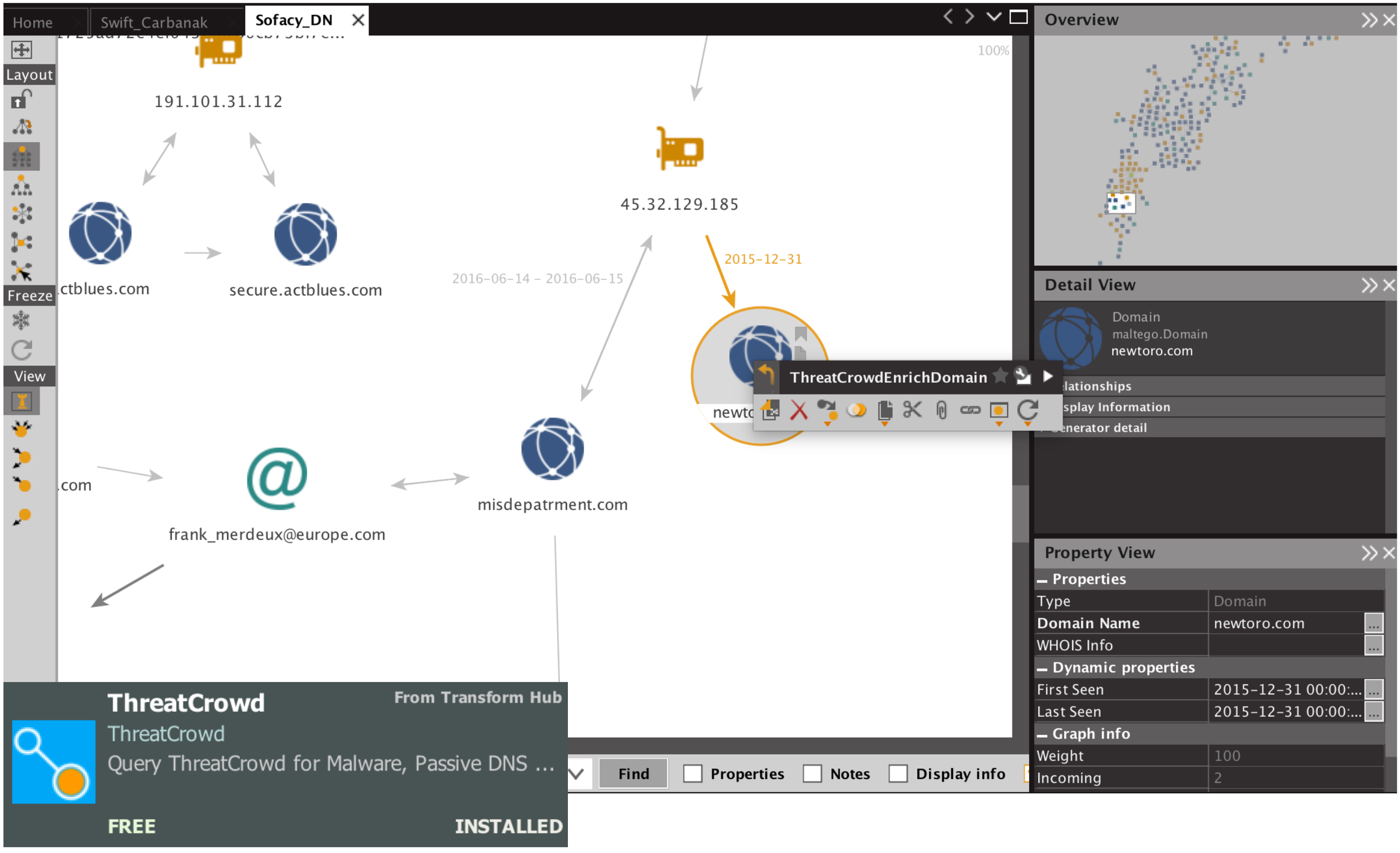
google.com?

RSS

https://www.threatcrowd.org/rss/index.php?query=dridex&type=antivirus

```
<?xml version="1.0" encoding="utf-8" ?>
<rss version="2.0">
<channel>
<title>ThreatCrowd RSS feed for dridex</title>
<link>http://www.threatcrowd.org</link>
<description><![CDATA[ThreatCrowd RSS feed for dridex]]></description>
<item>
<title>577a7d323c03ae572a38c8297f0e7216</title>
<link>http://www.threatcrowd.org/malware.php?md5=577a7d323c03ae572a38c8297f0e7216</link>
<description><![CDATA[MD5,577a7d323c03ae572a38c8297f0e7216,https://totalhash.cymru.com/analysis/?0035161ba2ebf562ae357c09374de389e99beb09]]></description>
</item>
<item>
<title>766098f8217e88664713185c4fb516e5</title>
<link>http://www.threatcrowd.org/malware.php?md5=766098f8217e88664713185c4fb516e5</link>
<description><![CDATA[MD5,766098f8217e88664713185c4fb516e5,https://malwr.com/analysis/NmE5YThkMmIzZDcwNGQ2YzkwNTNlOTA5NWZkMjBjYmU/]]></description>
</item>
<item>
<title>401a1021773f783c665b83a644a70fdf</title>
<link>http://www.threatcrowd.org/malware.php?md5=401a1021773f783c665b83a644a70fdf</link>
<description><![CDATA[MD5,401a1021773f783c665b83a644a70fdf,https://malwr.com/analysis/Y2RjYjEwOGI4YThmNDhmNjk0MmRmODI4YTg2NjVlNzQ/]]></description>
</item>
```

Maltego


Home
Swift_Carbanak
Sofacy_DN
Layout
Freeze
View
191.101.31.112
ctblues.com
secure.actblues.com
45.32.129.185
2016-06-14 - 2016-06-15
2015-12-31
100%
.com
frank_merdeux@europe.com
misdepatrment.com
ThreatCrowdEnrichDomain
Overview
Detail View
Domain
maltego.Domain
newtoro.com
lationships
splay Information
enerator detail
Property View
Properties
Type
Domain
Domain Name
newtoro.com
WHOIS Info
Dynamic properties
First Seen
2015-12-31 00:00:...
Last Seen
2015-12-31 00:00:...
Graph info
Weight
100
Incoming
2
Find
Properties
Notes
Display info
ThreatCrowd
From Transform Hub
ThreatCrowd
Query ThreatCrowd for Malware, Passive DNS ...
FREE
INSTALLED

API

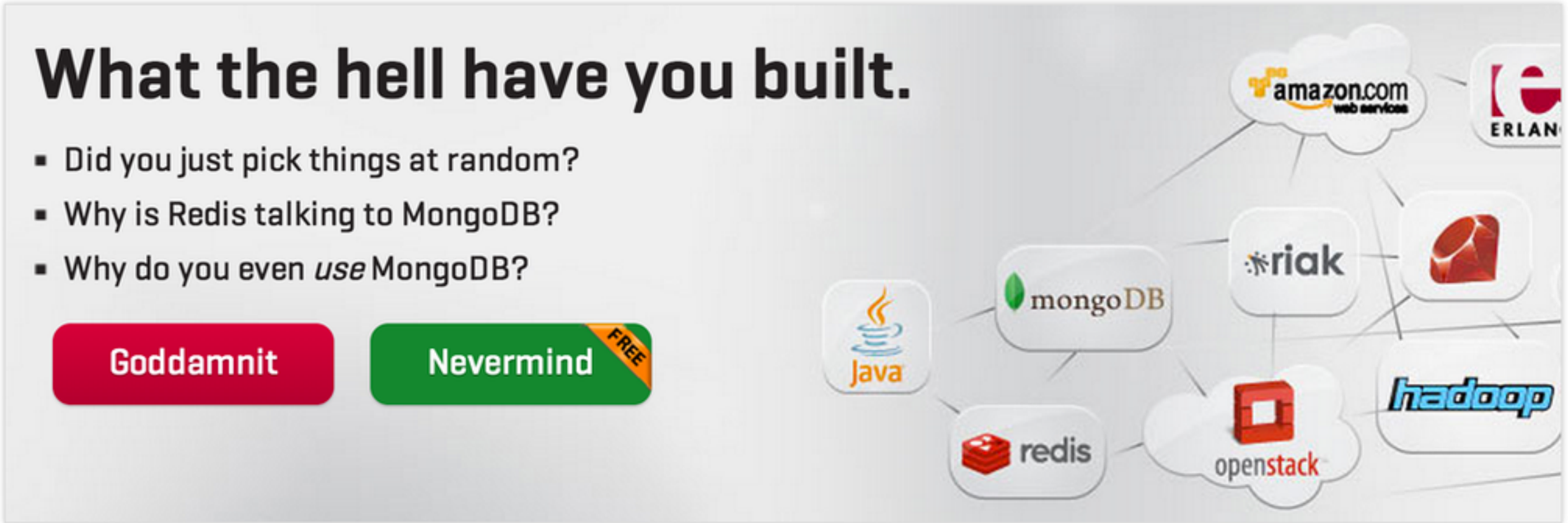
- Python pypi Library - https://pypi.python.org/pypi/threatcrowd
- Go package - https://github.com/jheise/gothreat
- Splunk Application - https://splunkbase.splunk.com/app/1657/
- Web application - https://ipintel.io/
- Python application - https://github.com/QTek/QRadio
- RabbitMQ - http://stoq.punchcyber.com/docs/
- Buatapa - http://www.brimorlabsblog.com/2015/08/publicly-announcing-buatapa.html
- Command line - https://github.com/jheise/threatcmd
- Splunk Application 2 - https://splunkbase.splunk.com/app/3081/
- R Package - https://github.com/threatcrowd/ApiV2/tree/master/RExample


```
{
  "response_code": "1",
  "domains": [
    "aoldaily.com",
    "aunewsonline.com",
    "cnndaily.com",
    "usnewssite.com"
  ],
  "references": [

  ],
  "permalink": "https:\/\/www.threatcrowd.org\/email.php
?email=william19770319@yahoo.com"
}
```


https://www.threatcrowd.org/searchApi/v2/email/report/?email=william19770319@yahoo.com

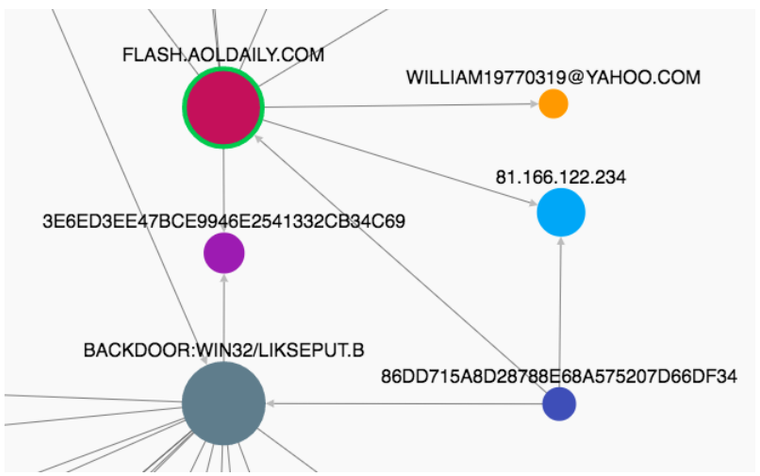
What is it built on?



via [boundary.com]

No magic here

+ cytoscape.js



You can access graph data easily with:
SQL + pivot(indicator)

Datasources are internal &

thanks!

Why should you build a free platform?

- You get to see Belfast
- You get to use it

~2014

+ some more

~2016

ThreatMiner
Data Mining for Threat Intelligence

OPEN THREAT EXCHANGE

IBM X-Force Exchange

AUTOFOCUS™

CYMON.IO

virustotal

MISP Threat Sharing

MALTEGO

PASSIVE TOTAL

CRITS

Palantir

THREATCONNECT™

+ loads more

A couple of tricks…

Search IOC | Search APTNotes

Credit: This is driven by a fork of the excellent APTNotes repository and all indicators ar

nuclear

2008 2009 2010 2011 2012 2013 2014 2015 2016

Search results for 'nuclear'

Kaspersky_Lab_crouching_yeti_appendixes_eng_final.pdf

Branch: master ▾ **signature-base** / **threatintel** /

Neo23x0 First Signature Set

..

get-misp-iocs.exe

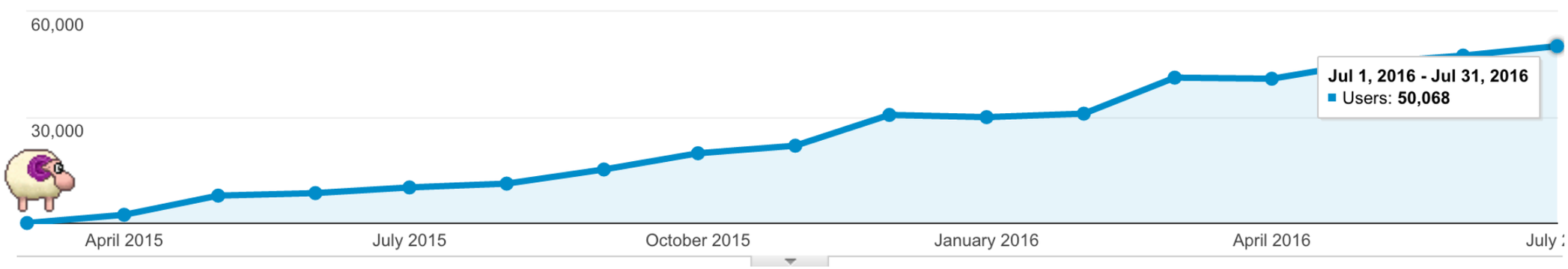
get-misp-iocs.py

get-otx-iocs.exe

get-otx-iocs.py

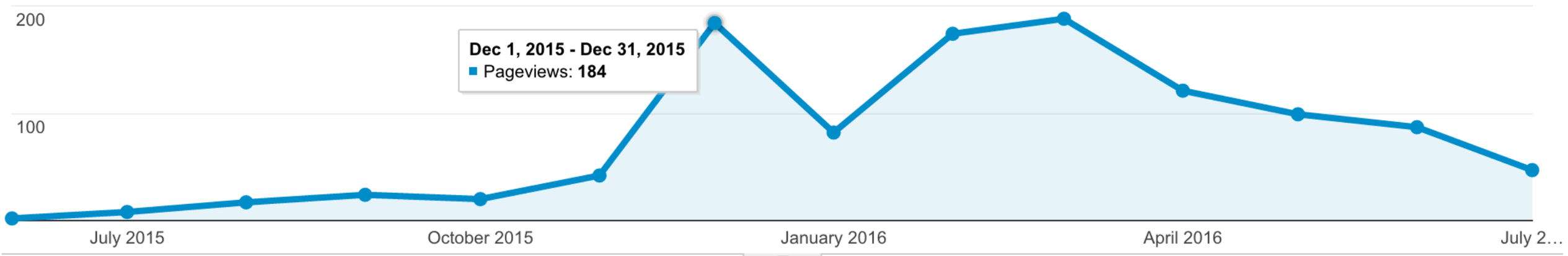
Who is using ThreatCrowd?

Stats

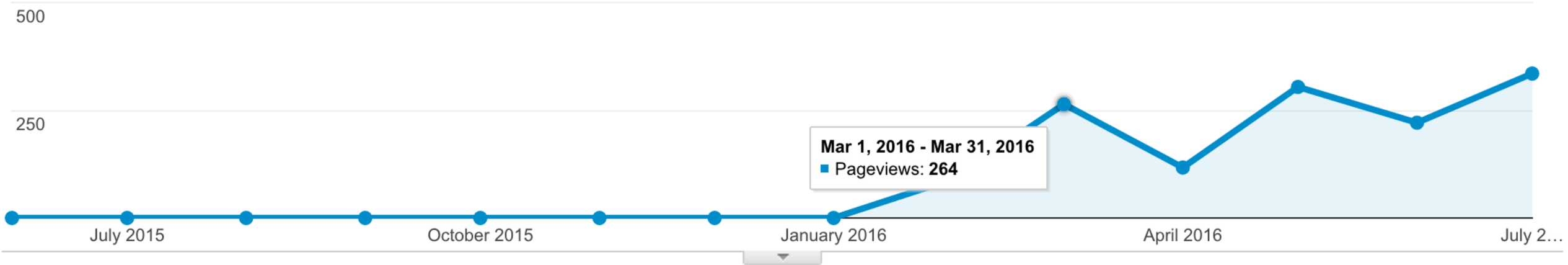


OPSEC?

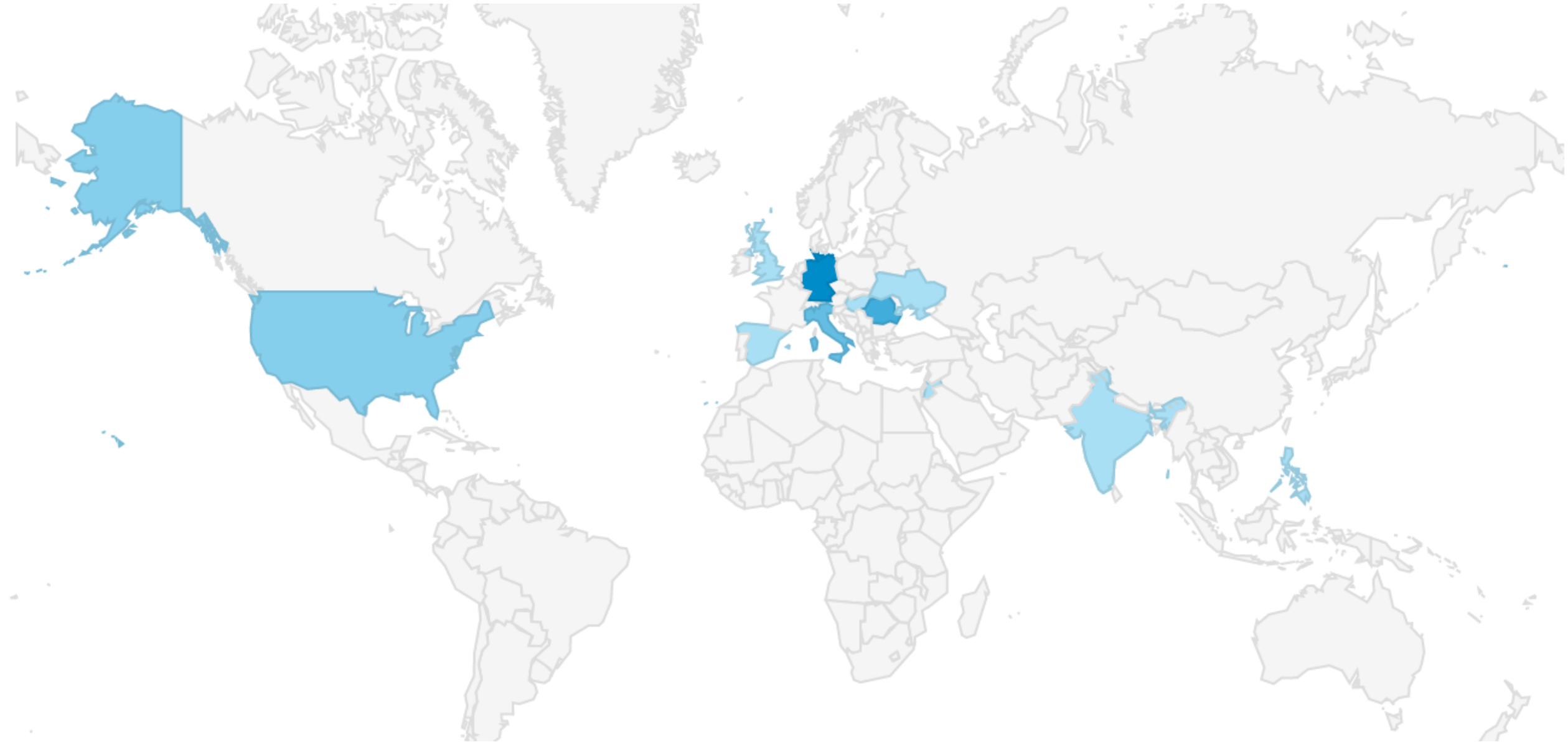
Dridex



Locky



antivirus.*(\.sofacy|sofacy\.)



Issues

SIGN UP

DOMAIN > DNSHOST.JUMPINGCRAB.COM

Most users have voted this as not malicious

Is this malicious? Yes No

FILES THAT TALK TO DNSHOST.JUMPINGCRAB.COM

MD5	A/V
5e3d6310d4670bc75c8b3c2a17b83d09	

WHY IS MY WEBSITE ON YOUR WEBSITE??

07:34:12.202867 IP 61.0.188.30.53 > 45.56.120.93.4444: 37110| 20/0/1 MX stagg.cpsc.gov. 5, MX hormel.cpsc.gov. 5, TXT "v=spf1 ip4:63.74.109.6 ip4:63.74.109.10 ip4:63.74.109.20 mx a:list.cpsc.gov -all", A 63.74.109.2, AAAA 2600:803:240::2, DNSKEY, DNSKEY, DNSKEY, DNSKEY, Type51, RRSIG[|domain]
07:34:12.229461 IP 61.0.188.30 > 45.56.120.93: ip-proto-17

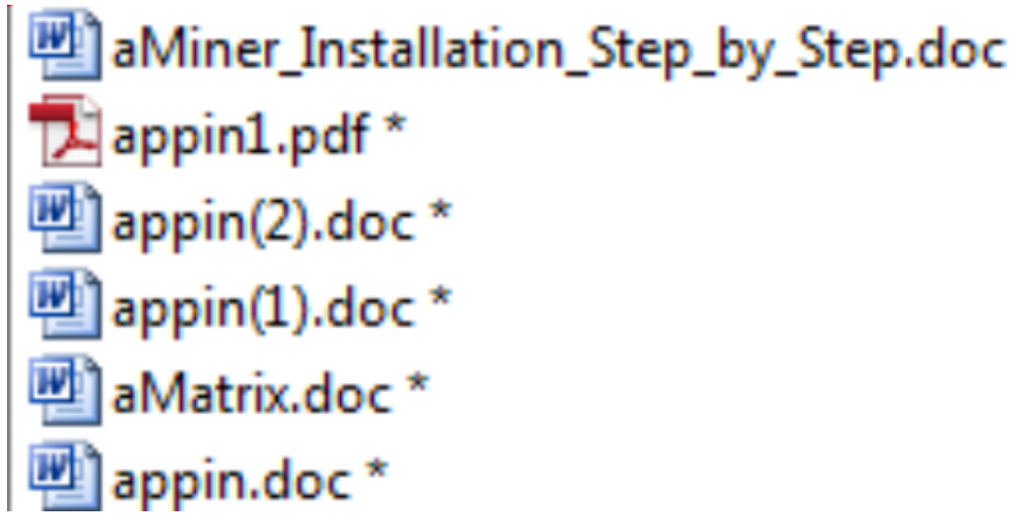
Where is ThreatCrowd going?
- Lots of change since ThreatCrowd was built in 2014
- Use case #1 - ThreatIntel – has changed

2013 - Tracking Hangover

D:\Projects\Elance\AppInSecurityGroup
\FtpBackup\Release\Backup.pdb

```
Registrant:
    Appin Technologies
    Rakesh Gupta          (rakesh.gupta@appinonline.com)
    9th Floor, Metro Heights,NSP, PitamPura,
    Delhi
    Delhi,110034
    IN
    Tel. +91.1147063300

Creation Date: 21-Apr-2010
Expiration Date: 21-Apr-2011
```



Via Nii Consulting and Norman Shark

2016 – Still Hangover?

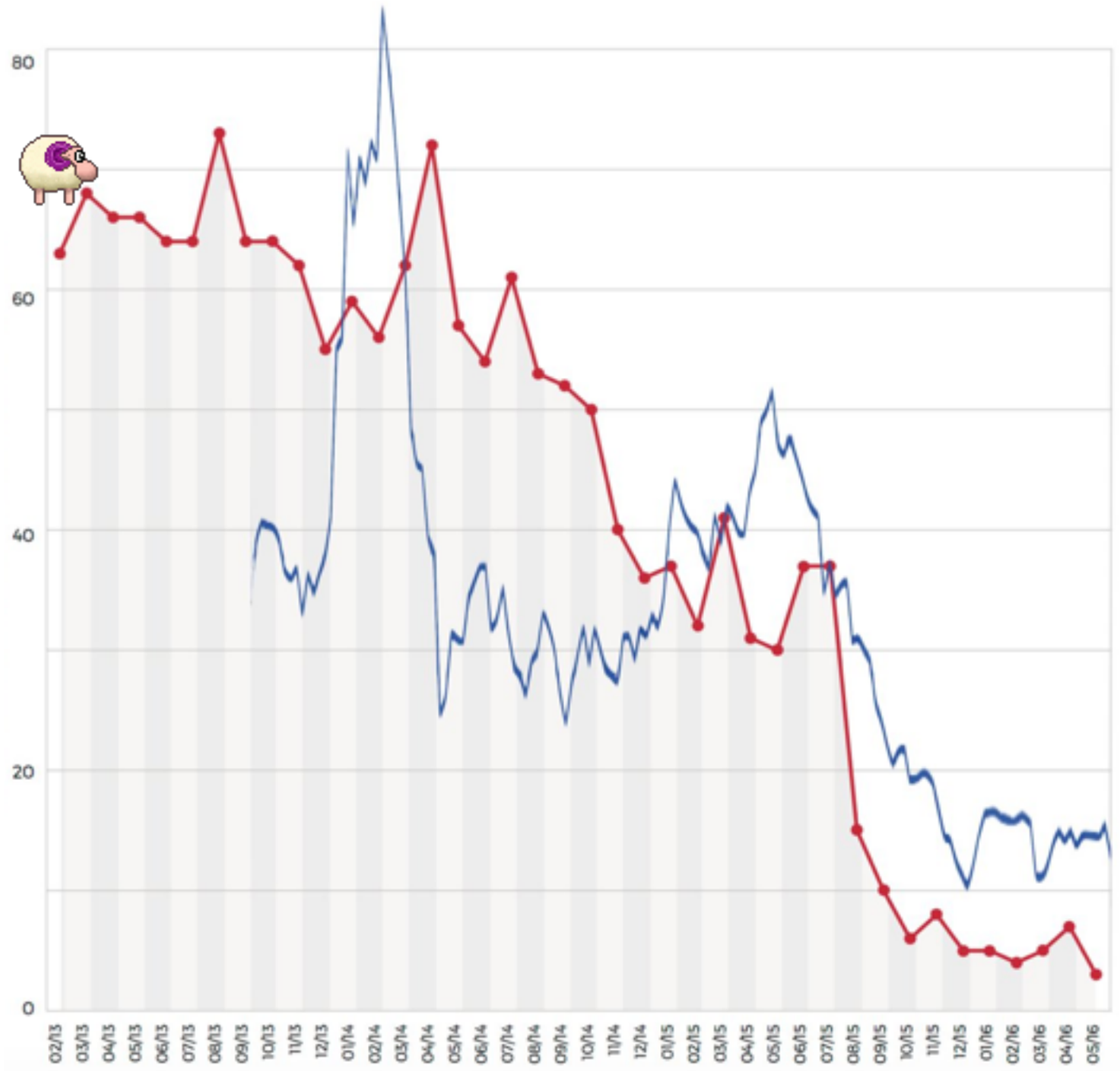
Via Cymmetria

Some things are getting harder to track

HUNTING THREAT ACTORS WITH TLS CERTIFICATES

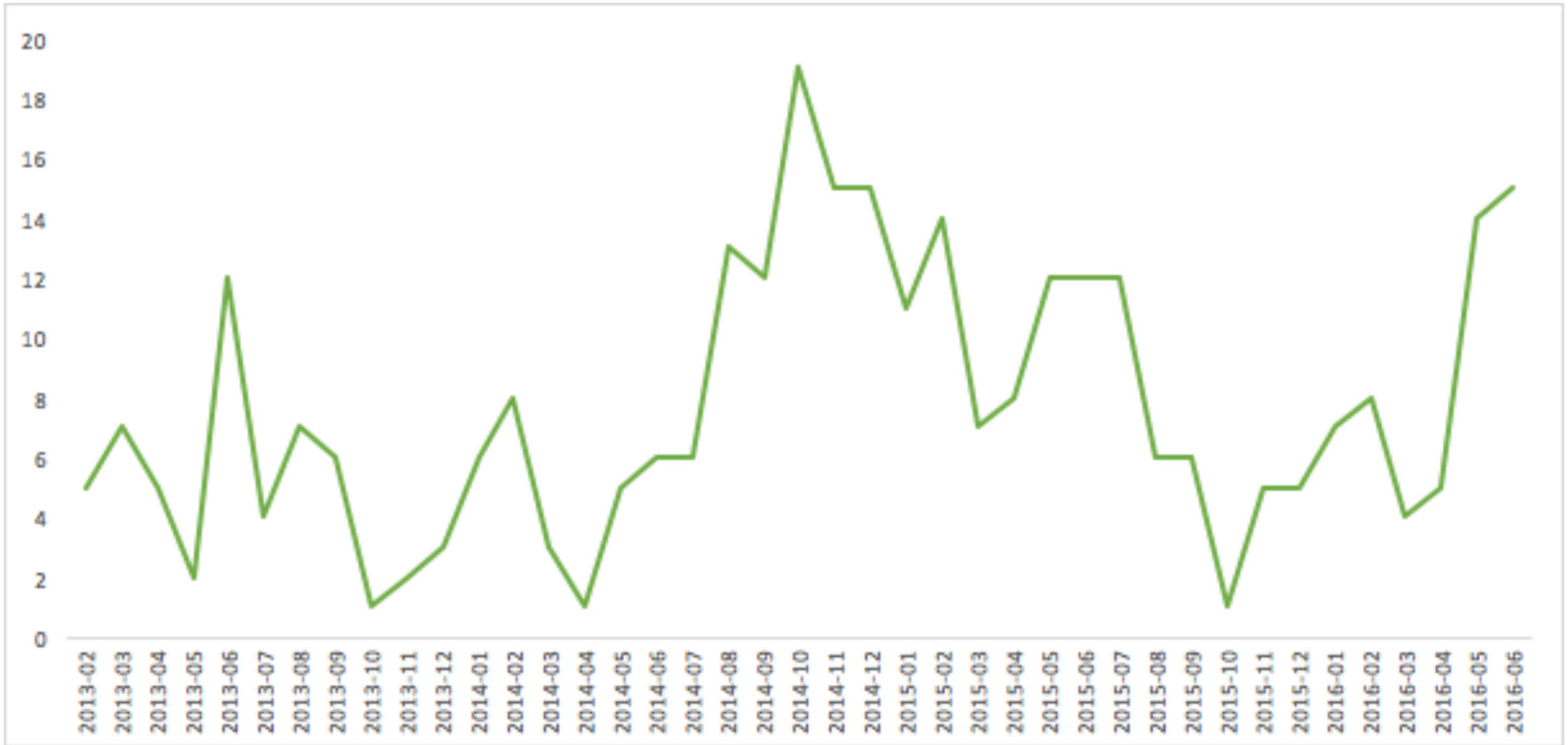
https://mpars0ns.github.io/bsidescharm-2016slides/

Are there still attackers worth tracking?



Via @daveaitel and @fireeye. * correlation != causation

Marketing doesn't show a drop in attackers worth tracking…



Via @APTNotes

… not that you can trust all the marketing

Norse Corp: Deconstructing threat intelligence on Iran

↓

Opinion: Security firm's Iran report mostly hype

APT28 TARGETS FINANCIAL MARKETS

ROOT9B RELEASES ZERO DAY HASHES

↓

Security Firm Redefines APT: African Phishing Threat

New evidence Sony hack was 'inside' job, not North Korea

Researcher: Sony hackers used fake emails

12 years old and finally over: Is the Harkonnen Operation the longest-running malware campaign so far?

Cyber-criminals targeting European corporations and governments managed to stay undetected since 2002 - until one security company found them.

↓

"Consumer Benefit Ltd" adware sites to block

IBM Trusteer research found that an average of 1 in 500 machines worldwide is infected with massively distributed APT malware at any point in time.

Still lots of activity worth tracking

Chinese hacking against Russian targets is on the rise

DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach

Exclusive: SWIFT warns customers of multiple cyber fraud cases

'Massive' Locky ransomware campaign targets hospitals

FORGET APT, MASS MALWARE IS STILL THE BIG THREAT

Via Bloomberg, FIRST, Guardian

Already some great resources for crimeware

Recent Locky Malspam IoCs from Malware Traffic Analysis

CREATED 10 DAYS AGO neonprimetime 0 COMMENTS

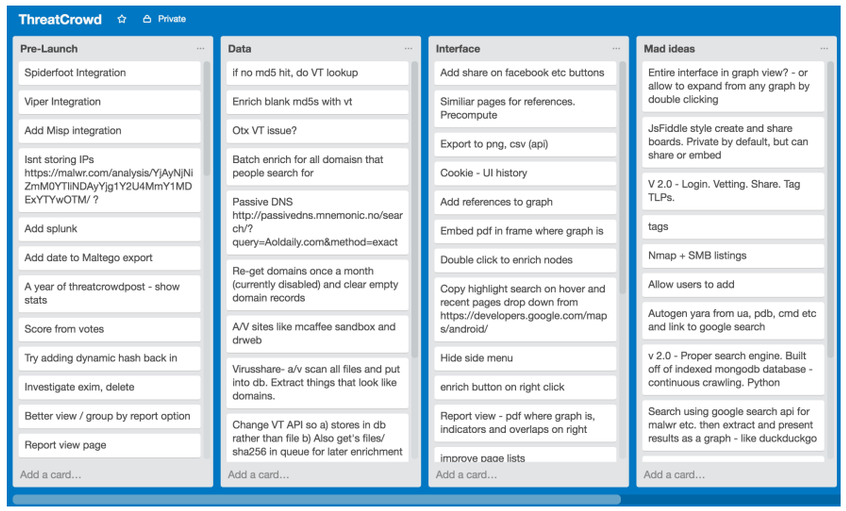
Recent Locky Malspam IoCs from Malware Traffic Analysis Found by @malware_traffic not me 7/23/16 to 8/18/2016

15 SUBSCRIBERS 0 VOTES

MALSPAM LOCKY MALWARE TRAFFIC ANALYSIS

Dateadded (UTC)	Threat	Malware	Host (?)
2016-08-27 18:01	Botnet C&C	Locky	wvltrlrnf.xyz
2016-08-26 08:38	Distribution Site	Locky	www.caffematto.it

Where is ThreatCrowd going?



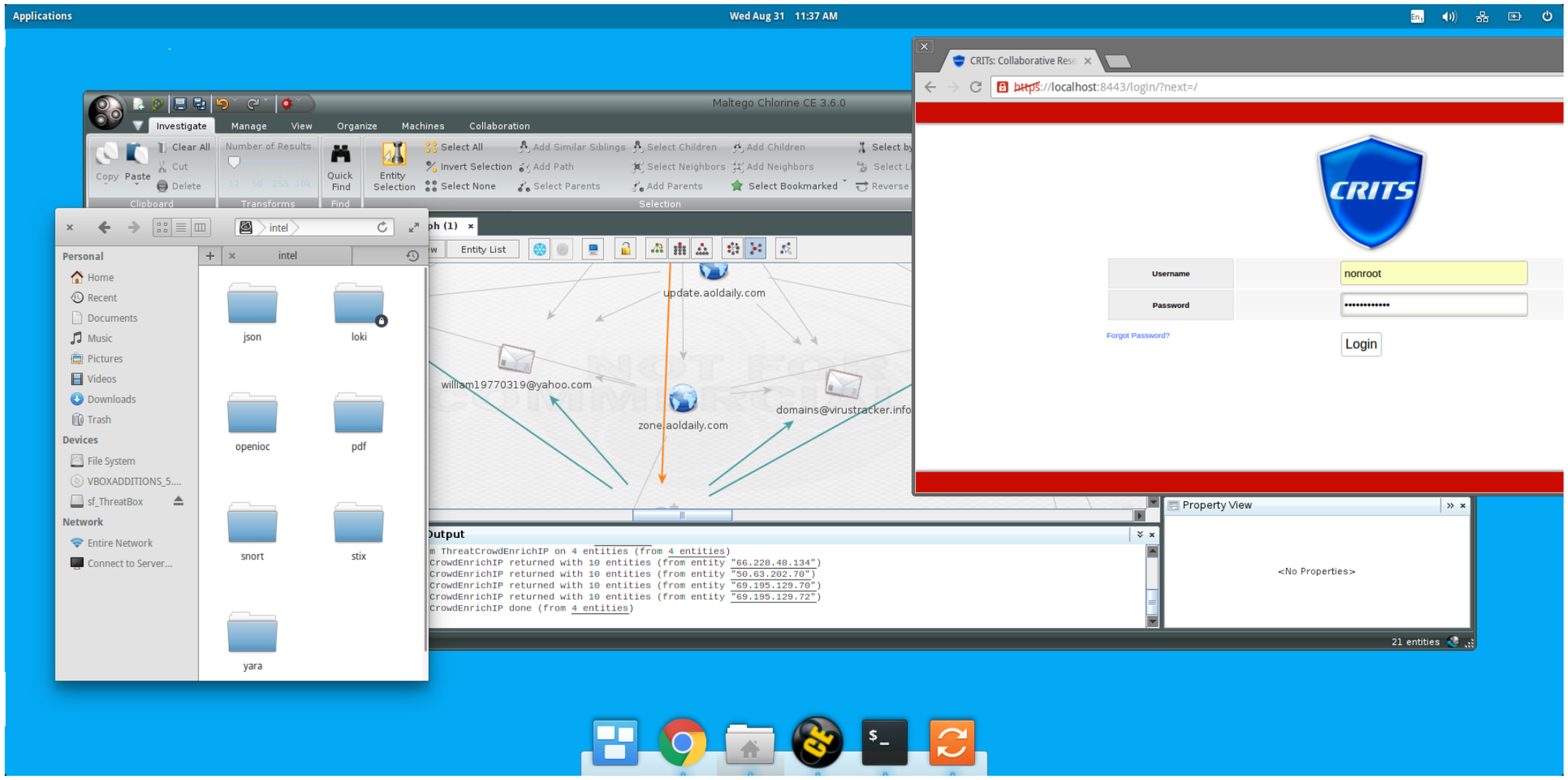
We don’t need another commercial platform

Lots of hosting offers from the community - thanks!

May hand over to the community

What do you think?

Coming Soon - ThreatBox(?)



Reduce the infosec echo chamber - try tools quickly

Integrate the free intel with tools to apply it

SIFT & Remnux are awesome but different

Want to beta test?

Questions?

@chrisdoman / threatcrowd.org

vectranetworks.com