RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: HT-R11

Hunt Advanced Attackers on a Budget Less than the GDP of a Small Country

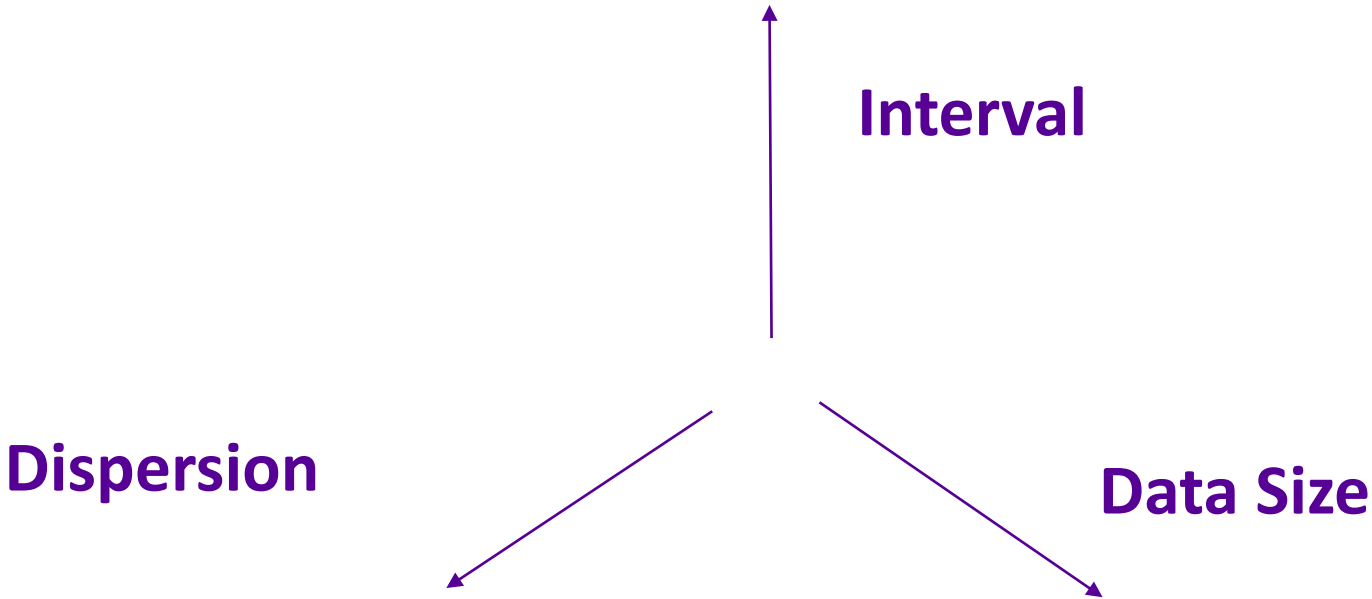
John Strand
Owner
Black Hills Information Security
@strandjs

Hunt Advanced Attackers on a Budget Less than the GDP of a Small Country

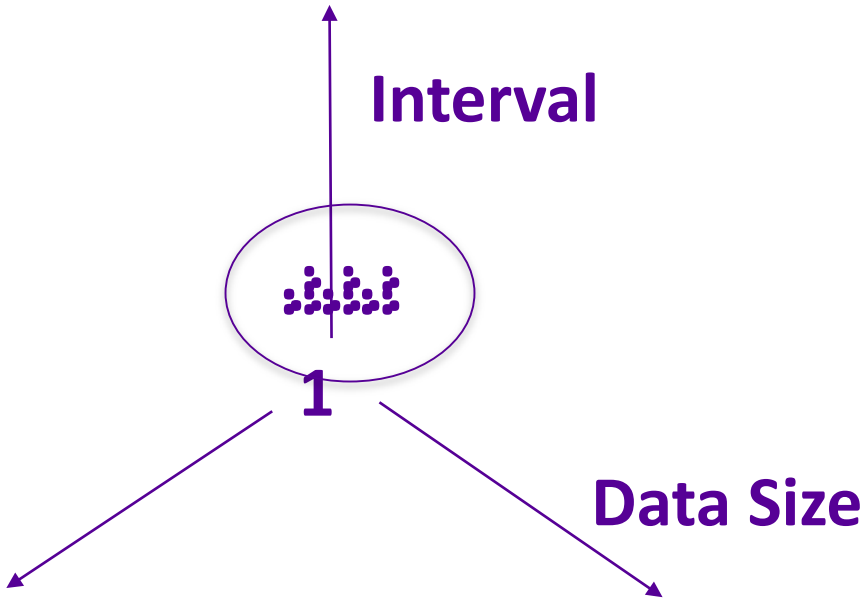
Problem: Detecting Command and Control is getting hard

- There are a number of backdoors that use a wide variety of different ways to communicate with the bad guys' Command and Control (C2) servers
  - HTTP Beaconing
  - Social Media
  - DNS
  - QUICK
  - SCTP
- PenTesting firms use these tricks all of the time
- As do the bad guys
- How can we detect these backdoors if the data is encrypted, obfuscated or hidden?
- We can use AI
  - Please.. Don't stop watching just yet...

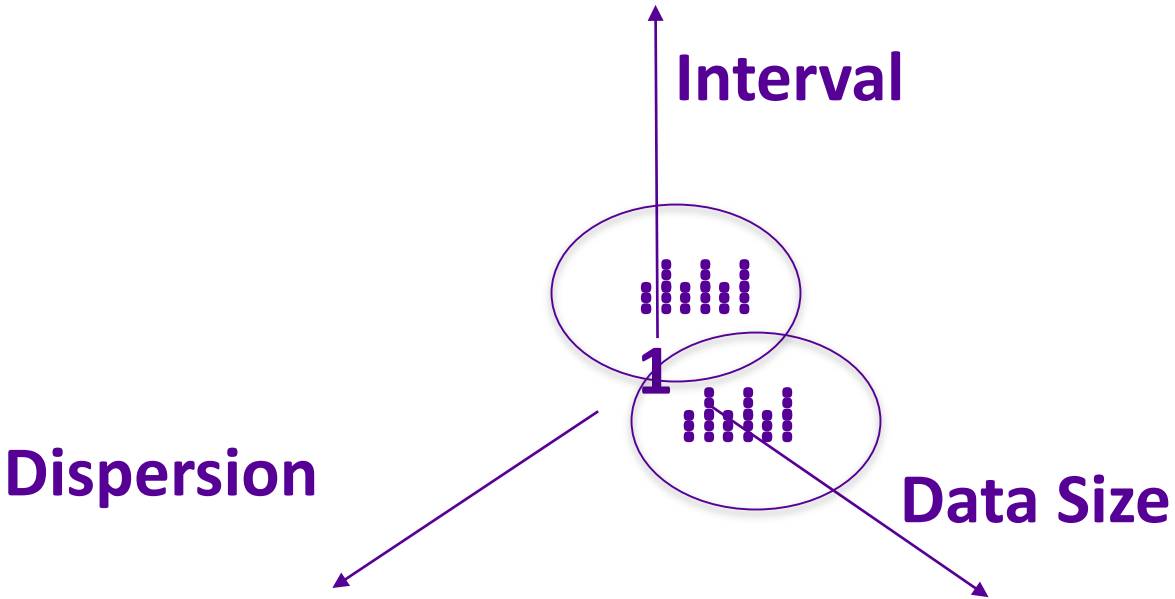
Let's think about consistencies.



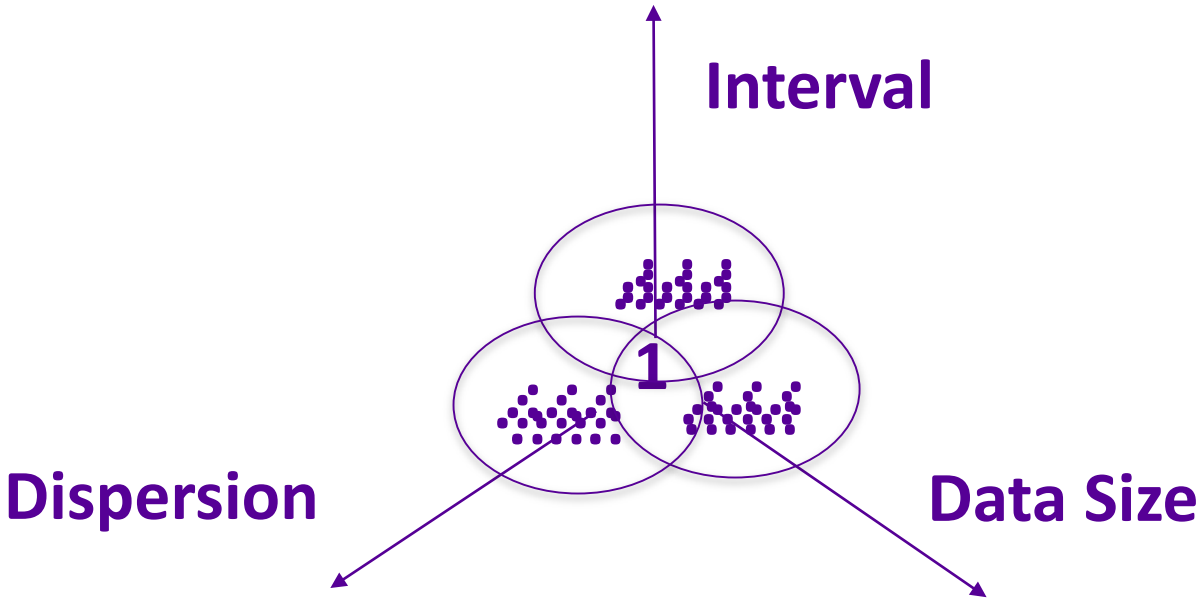
Let's think about consistencies.



Let's think about consistencies.

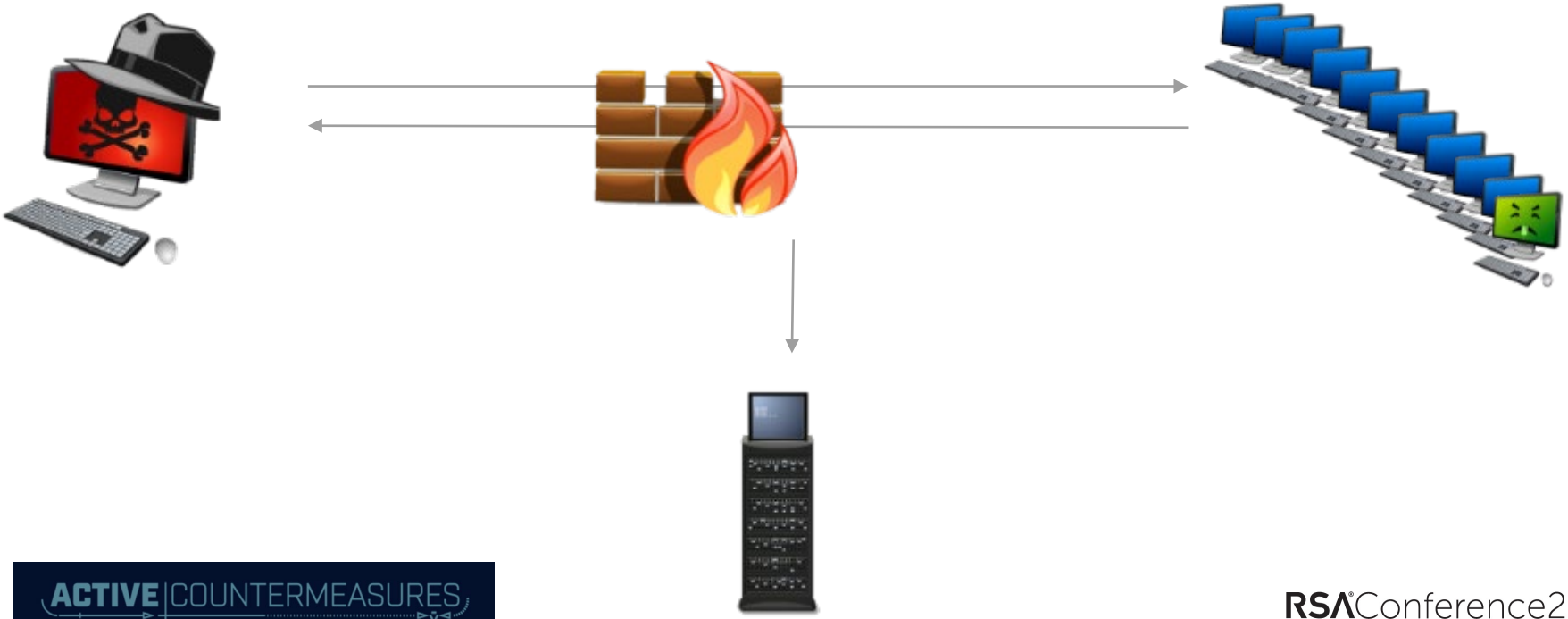


Let's think about consistencies.



Let's talk about setup

- First, you will need to have a system to capture the traffic
- Second, RITA is free and awesome

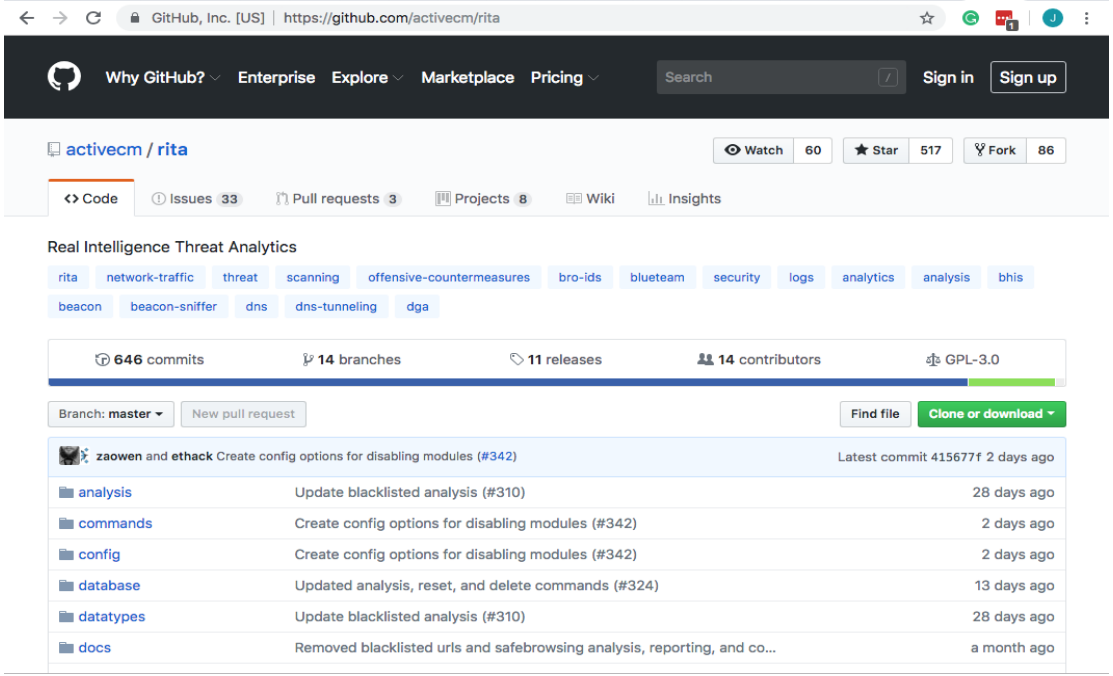


Why Zeek?

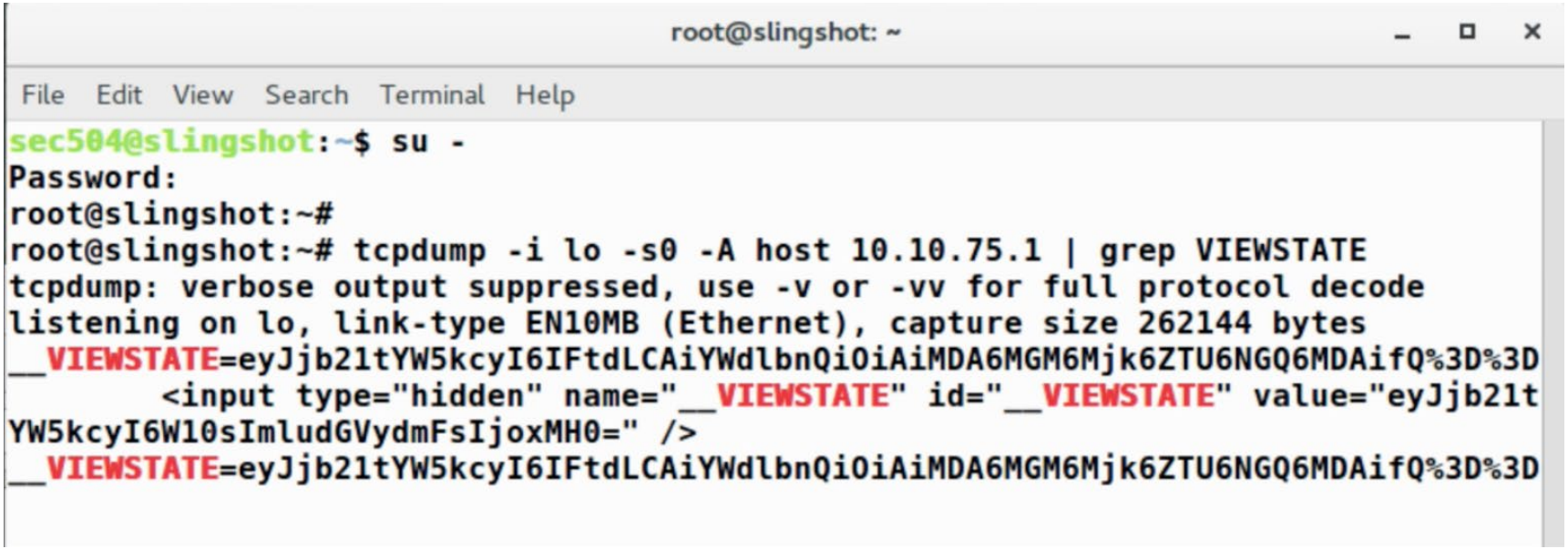
- Speed
- Large user base
- Lots of support
- Consistency
  - Timestamps are key
  - Many devices handle timestamps in different/odd ways
  - Generates required log files
- We are moving away from signature-based detection
- Too many ways to obfuscate
  - Encryption, Encoding, use of third-party services like Google DNS

RITA is free… It is also the source of most of the data we will cover:

https://www.activecountermeasures.com/rita/



VSAgent


root@slingshot: ~
File Edit View Search Terminal Help
sec504@slingshot:~$ su -
Password:
root@slingshot:~#
root@slingshot:~# tcpdump -i lo -s0 -A host 10.10.75.1 | grep VIEWSTATE
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
__VIEWSTATE=eyJjb21tYW5kcyI6IFtdLCAiYWdlbnQiOiAiMDA6MGM6Mjk6ZTU6NGQ6MDAifQ%3D%3D
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="eyJjb21t
YW5kcyI6W10sImludGVydmFsIjoxMH0=" />
__VIEWSTATE=eyJjb21tYW5kcyI6IFtdLCAiYWdlbnQiOiAiMDA6MGM6Mjk6ZTU6NGQ6MDAifQ%3D%3D

DNSCat

sec504@slingshot: ~/tools/Enterprise_Lab/DNSCat_Logs/2017-03-20

File Edit View Search Terminal Help

```
dp      242464a1b01050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 71d501050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072389.346211  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      29202443d01050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 e92601050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072390.526357  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      6087340401050c0d05fbab.cat.nanobotninjas.com 1       C_INTERNET      16      TXT     0       NOERROR F
        F       T       T   0TXT 18 f54401050cfbab0d05      59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072391.702286  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      155730be301050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 1b3001050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072392.882308  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      317357fe401050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 6e4201050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072394.062274  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      22968232b01050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 4fa401050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072395.234214  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      20977764601050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 5b4401050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072396.406238  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      19052152101050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 4d9201050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072397.578267  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      2343569a701050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 83e701050cfbab0d05       59.000000       F
dns.23:00:00-00:00:00.log.gz:1490072398.754334  CbEtxF16rCk0utMKw2      10.234.234.105  56122   8.8.8.8 53      u
dp      10007305201050c0d05fbab.cat.nanobotninjas.com        1       C_INTERNET      16      TXT     0       NOERR
OR F        F       T   T0       TXT 18 844001050cfbab0d05       59.000000       F
$
```

Housekeeping: Ads

- Ads… Oh my… Ads
- You need to block them
- They bring malware
- They pollute the data

Round Robin Malware Beaconing

- We have been seeing malware that connects to multiple different IP addresses
  - QUIC
  - SCTP
- One giveaway is the datasize
- The IPs may shift, but the dispersion and the data size are still consistent
- Look for an internal system making connections to multiple external systems with the same attributes

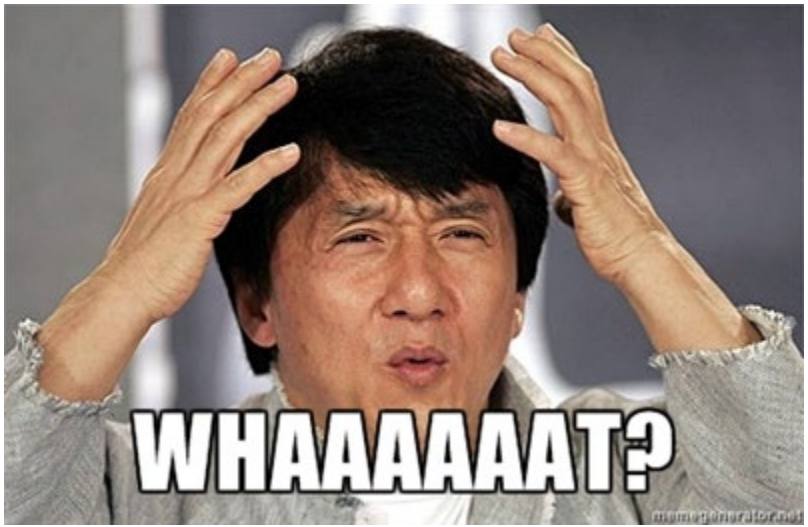
ACTIVE COUNTERMEASURES

What happens when your entire network is connecting to DoD?

- We had a customer who had a large (think thousands) of systems connecting to a DoD IP address on the Internet
- Very strong and consistent beacon
  - Datasize
  - Dispersion
  - Interval
- Time to panic?
- Is the NSA hacking them?
- Was it a Vault or ShadowBroker exploit?
- Made no sense at all…..

Quote from a developer…

"Wait… That IP address is odd.. It is the current version of product X."



Lesson

- Sometimes “beaconing” data is not evil
- Sometimes it is just a mistake
- Trust me, there are lots of mistakes on networks….
  - Syslog from products
  - “Customer experience data”
  - Direct Software updates trying to get to the Internet
- There is a lot of filtering and research when you first do this
- But, it gets easier
- Think Vulnerability Assessments

Did someone say a “Touch of Evil?”

On the topic of blacklisting...

- There are multiple different sources of blacklisted IP/DNS information
- Most of them feed of each other
- Having a hit on a blacklist does not mean the connection is immediately evil
  - Virtual hosting
  - Old entries
- So, simply because a connection is made to an IP address does not mean the system is compromised

What to look for: Numerous hits

IP Blacklist Report

Engine	Help
MyWOT	More info
LAPPS Grid Blacklist	More info
MalwareDomainList	More info
TalosIntel IPFilter	More info
AlienVault Reputation	More info

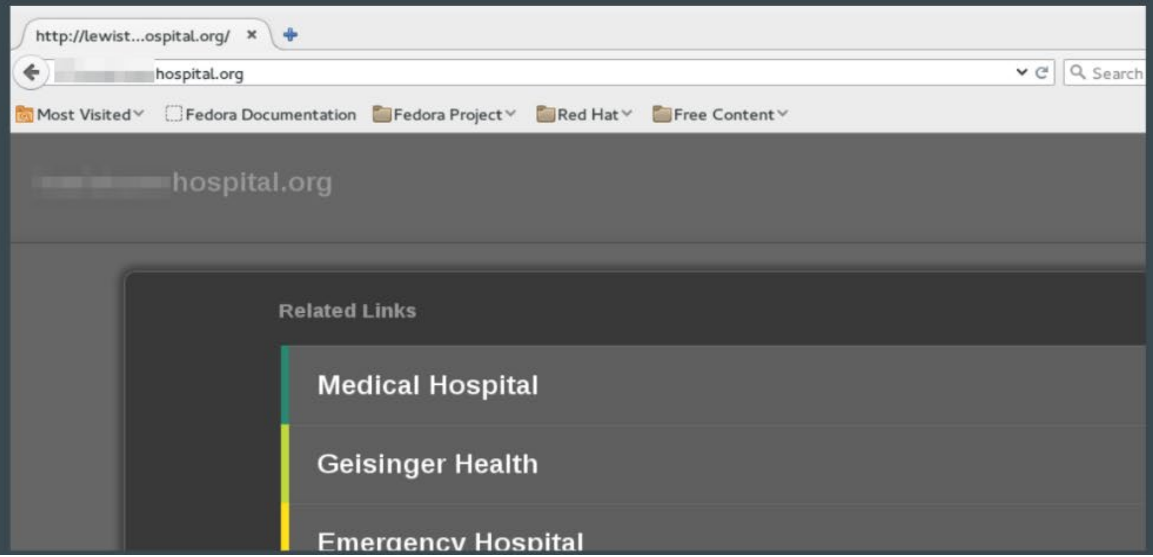
What to look for: Amount of data transferred

A note on porn

When good sites go bad...

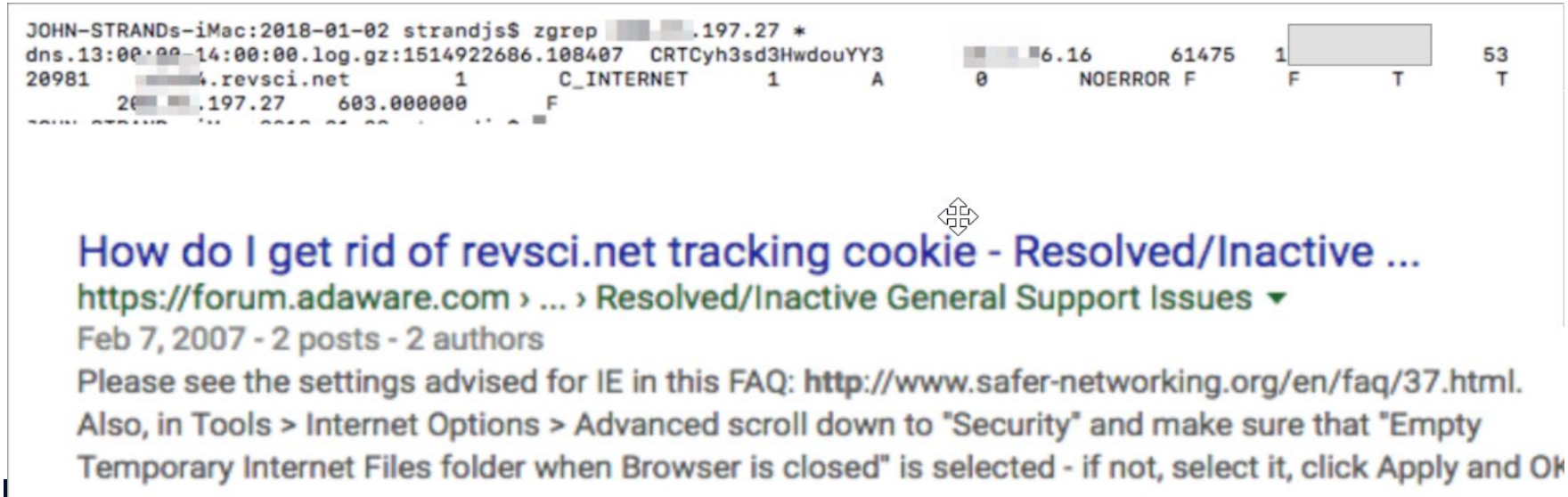
Seems legit..

```
dns.04_00_00-05_00_00.log.gz:1500625760.798530  C65C5q11z6AIUMOWFg      1[redacted].162    12037   172.16.48.7     53      udp     14947   0.04770
8       [redacted]hospital.org  1       C_INTERNET      1       A       0       NOERROR F       F       T       T       1       204.11.56.48  3
00.000000       F
```



Spyware is…. Weird

- Not quite ad… Not quite malware…
- Usually used for tracking a user
- All advertisers do this



Compromised Servers

```
$ nmap -p 0-65535 [redacted].170.149
Nmap scan report for [redacted].com ([redacted].170.149)
Host is up (0.025s latency).
Not shown: 49132 filtered ports, 16393 closed ports
PORT  STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
2082/tcp open  infowave
2083/tcp open  radsec
2086/tcp open  gnunet //GNUNet is a framework for P2P networking
2087/tcp open  eli //Event logging integration
2095/tcp open  nbx-ser
2096/tcp open  nbx-dir
2222/tcp open  EtherNetIP-1 Typing EtherNetIP-1 to google recommends
                            EthernetIP-1 service exploit
3306/tcp open  mysql
```

Crypto mining is the new hotness

```
ohn@AlteredCarbon:~$ nmap [redacted]4.81

tarting Nmap 7.60 ( https://nmap.org ) at 2018-01-22 13:47 MST
tats: 0:00:13 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
arallel DNS resolution of 1 host. Timing: About 0.00% done
map scan report for [redacted].174.81
ost is up (0.14s latency).
ot shown: 997 closed ports
ORT     STATE SERVICE
2/tcp   open  ssh
000/tcp open  ppp
080/tcp open  http-proxy

map done: 1 IP address (1 host up) scanned in 24.74 seconds
ohn@AlteredCarbon:~$
```


```
curl http:/[redacted]4.81:8080/list
[{"ip":"[redacted].212.20","workers":4,"power":30},{"ip"[redacted].181.204","workers":4,"power":30},{"i
p":[redacted]9.213","workers":4,"power":30},{"ip":"[redacted].223.138","workers":4,"power":30}]
```

Online Resource: IP/URL Void

IP Address Information

Analysis Date	2018-02-20 10:09:46
Elapsed Time	2 seconds
Blacklist Status	BLACKLISTED 4/96
IP Address	**104.27.163.228** Find Sites | IP Whois
Reverse DNS	Unknown
ASN	AS13335
ASN Owner	Cloudflare Inc
ISP	Cloudflare
Continent	North America
Country Code	(US) United States
Latitude / Longitude	37.751 / -97.822 Google Map

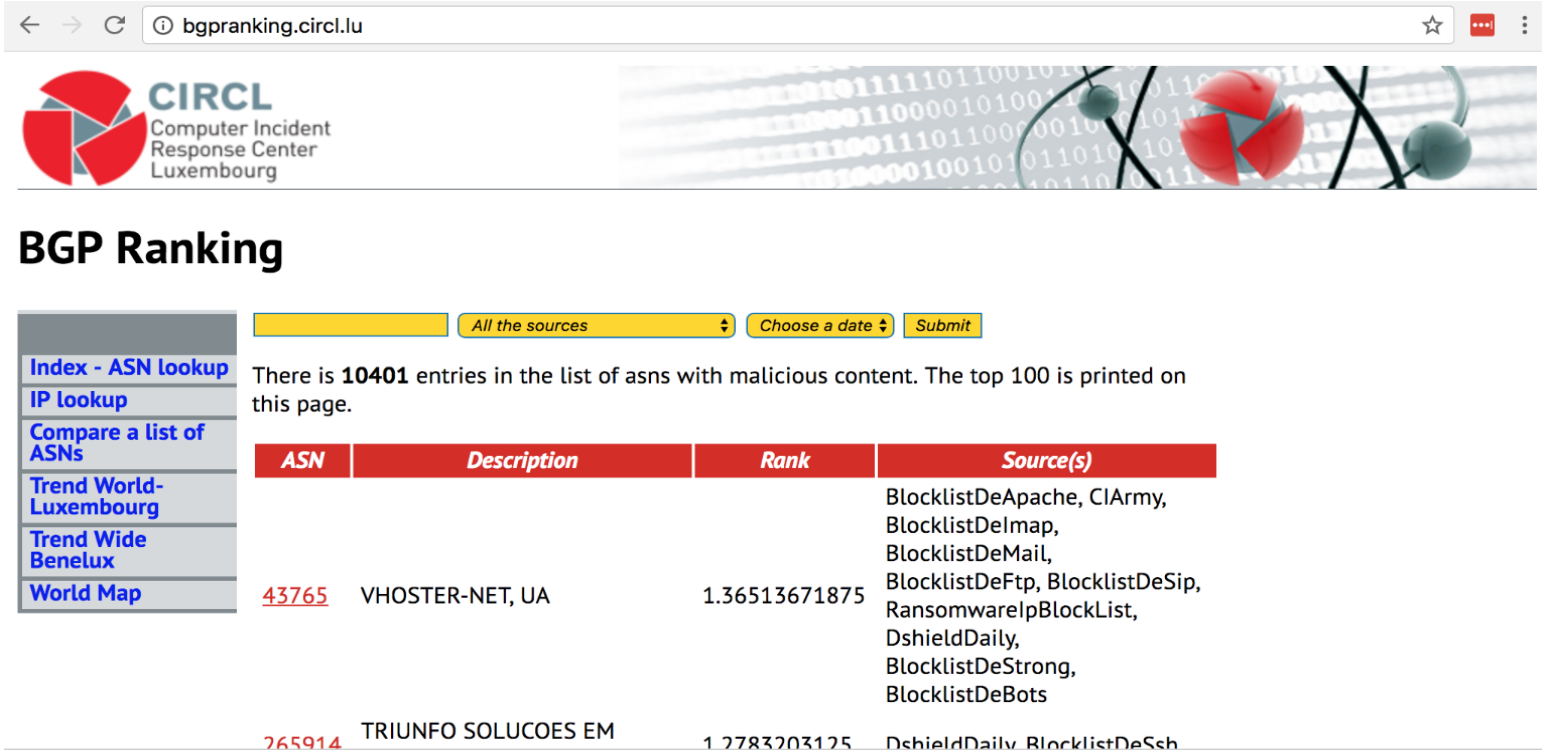
IP ADDRESS: 104.27.163.228

We have found in our database of already analyzed websites that there **are 14 websites** hosted in the same web server with IP address **104.27.163.228**. Remember that it is not good to have too many websites located in the same web server because if a website gets infected by malware, it can easily affect the online reputation of the IP address and also of all the other websites.

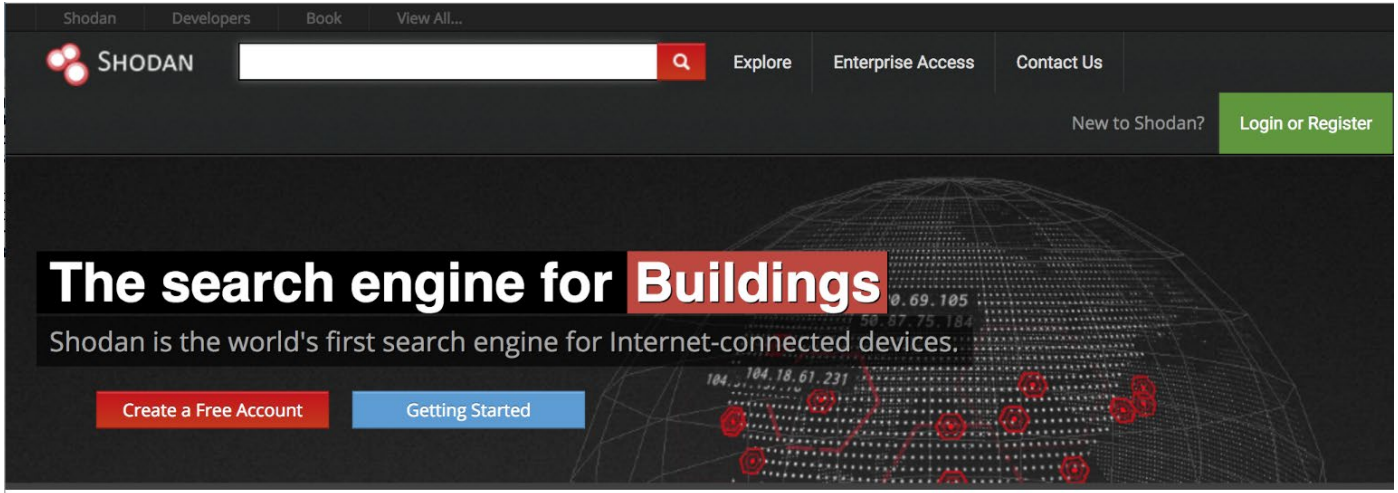
Browse a list of websites hosted in **104.27.163.228** IP address:

#	Website
1	✔ prototypo.io
2	✔ e-glasshouse.com
3	✔ alphabetawood.com
4	✔ prayoga.biz
5	✔ trendo-news.com

BGP/ASN Ranking



Shodan… Not just for pentesters...



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

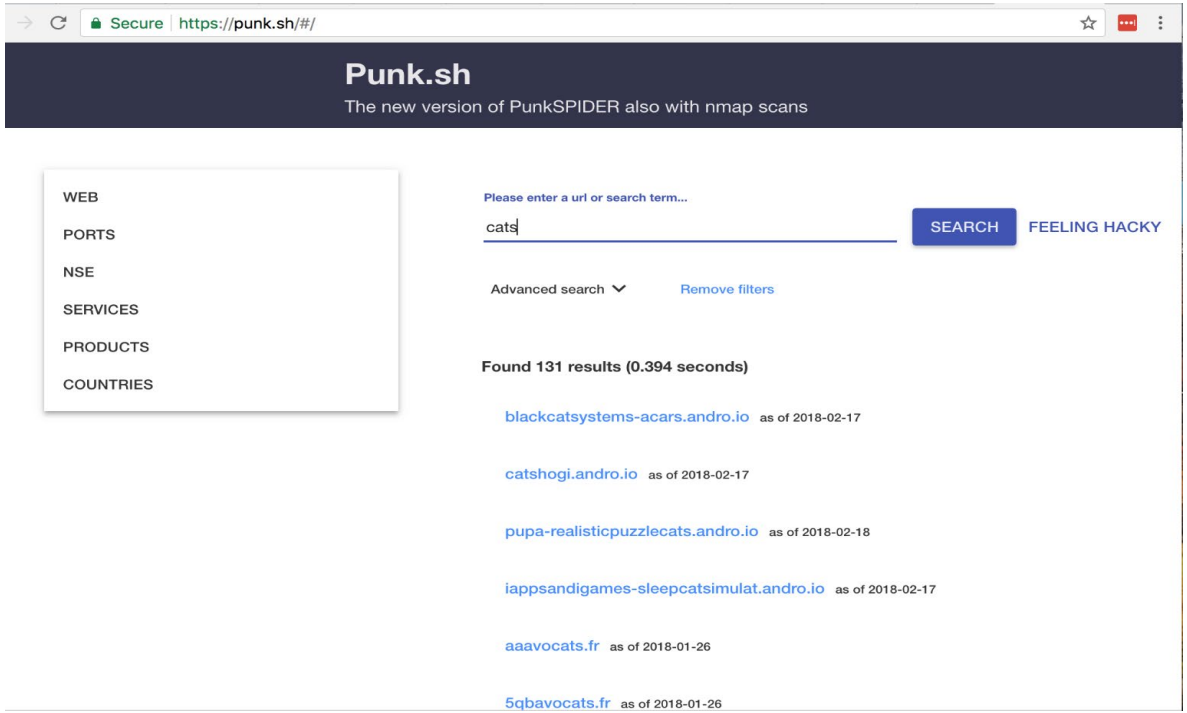
Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

PunkSPIDER is back!



Conclusions

- Detecting Command and Control traffic is getting harder and harder
- We released RITA to help detect some of the backdoors we use everyday
- *It is free. GO GET IT!*
- There are also a lot of free resources available to research network oddities
- Does require a bit of digging
- Odd != Evil
- Housekeeping is often required!
- Thanks!

ACTIVE COUNTERMEASURES

ACTIVE COUNTERMEASURES