Using Bro to Hunt Persistent Threats

Benjamin H. Klimkowski

United States Military Academy

13 September 2017

Agenda

1. Goals
2. Definitions
3. Motivating problem
4. Approach
5. How Cobalt Strike works
6. Traffic analysis
7. Evaluation
8. Results
9. Detecting other sets of activity
10. Future directions
11. Questions

Goals

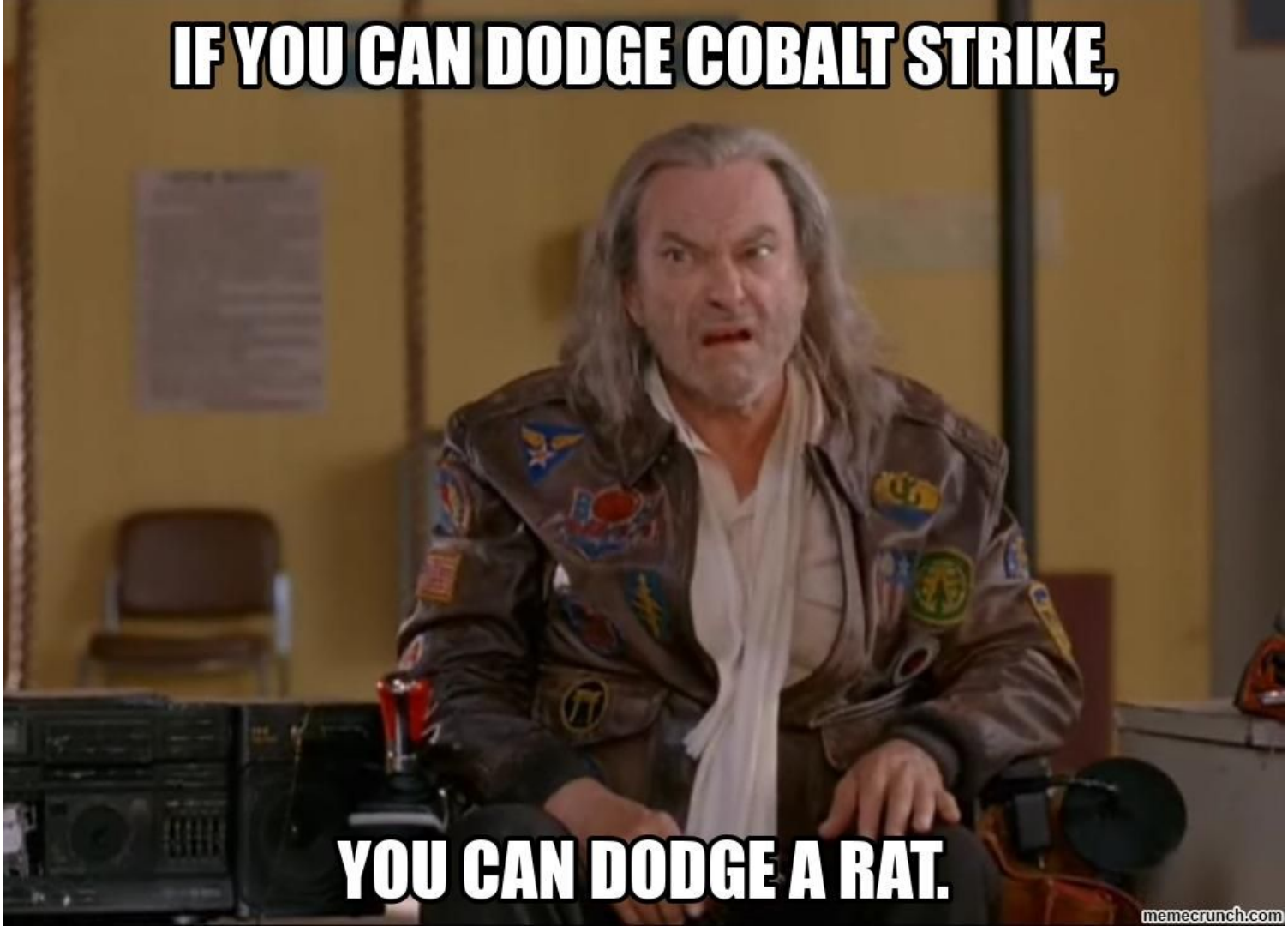
- Demonstrate how Bro supports analysis over different phases of hunting
- Discuss how persistent threat actors manipulate traffic to be stealthy
- Share insights about Bro in a live detection setting and part of larger security architecture
- Share some cool tools and techniques

Disclaimers

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the US Government.

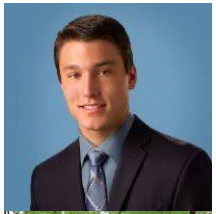
The focus of this presentation is the not pedagogical merit of defensive cyber exercises/competitions

This presentation is neither an indictment nor endorsement of Cobalt Strike


IF YOU CAN DODGE COBALT STRIKE,
YOU CAN DODGE A RAT.
memecrunch.com

who --all

- Undergraduate Team
  - Mitch Deridder



  - Dale Lakes

  - Matt Shockley

Senior Faculty Advisor

- W. Michael Petullo

whoami

- Professional
  - Cyber Protection Team Leader, Unites States Army Cyber Protection Brigade
  - Assistant Professor, Computer Science, United States Military Academy
  - Computer Network Operations Plans Officer, Army Cyber Command
  - Network Watch Officer, Army Cyber Operations and Integration Center
  - Infantry officer
- Education
  - MS, Computer Science, University of Maryland
  - MS, Telecommunications, University of Colorado Boulder
  - BS, Mechanical Engineering, United States Military Academy
- Research Interests: machine learning/data mining, network and host security, traffic analysis
- Father of three
- Weightlifting, MMA, reading

Definitions

- Persistent threat
  - High tradecraft
  - Well-resourced
  - Leverages vectors that hide/obscure initial access
- Hunting
  - “Proactive approach to identifying threats on network”
  - Threat-focused
  - Emphasis on data analysis to identify hard to find activity
  - May or may not be done in conjunction with incident response

Motivating Problem

- 2017 Cyber-Defense Exercise (CDX)
  - Sponsored by NSA
  - Blue forces: US and Canadian service academies compete
  - Participants design, build, and defend network
- NSA Red Team
  - Simulated persistent threat compressed to four day
  - Target blue user workstations and services via an automated scoring system
  - Pre-compromised images
  - White-cell induced client-side attacks
  - Timed Injects/challenges
- Defenders
  - Simulated SOC/NOSC/CERT
  - Part of larger architecture
  - Stiff availability penalties for loss of service and interaction with user workstations during competition

Attack Cycle

- Reconnaissance:
  - Passive and active reconnaissance
- Scanning and enumeration:
  - Identify systems, services, topology, etc.
- Gain initial access:
  - Software vulnerabilities
  - Weak passwords or configurations
  - Credential stealing, social engineering, insiders
- Escalation of privilege:
  - Sniffing, keylogging, active attack
- **Maintain access:**
  - **Compromised accounts, rootkits, remote access tools (RATs)**
- Cover Tracks:
  - Delete logs/ history

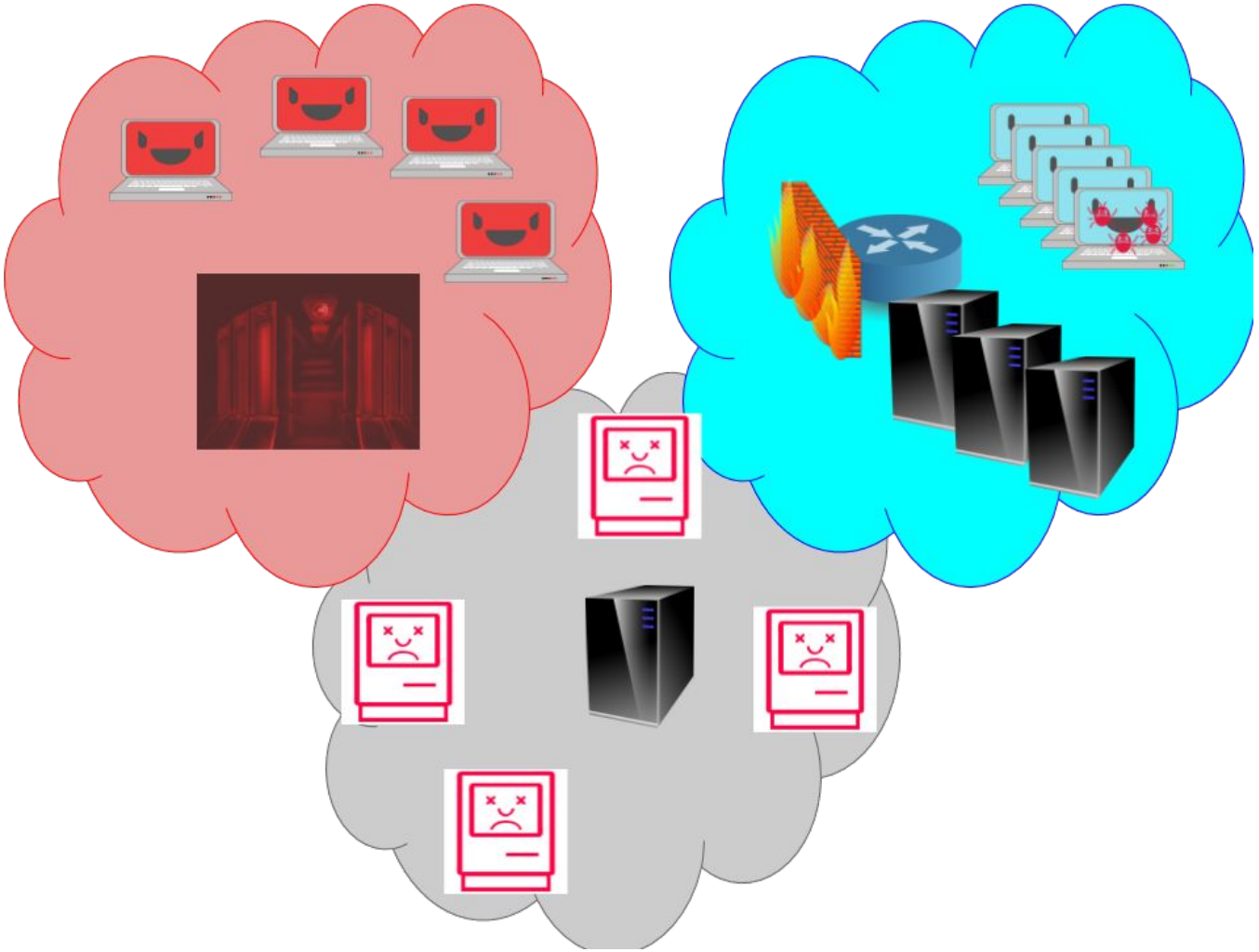
Our Approach

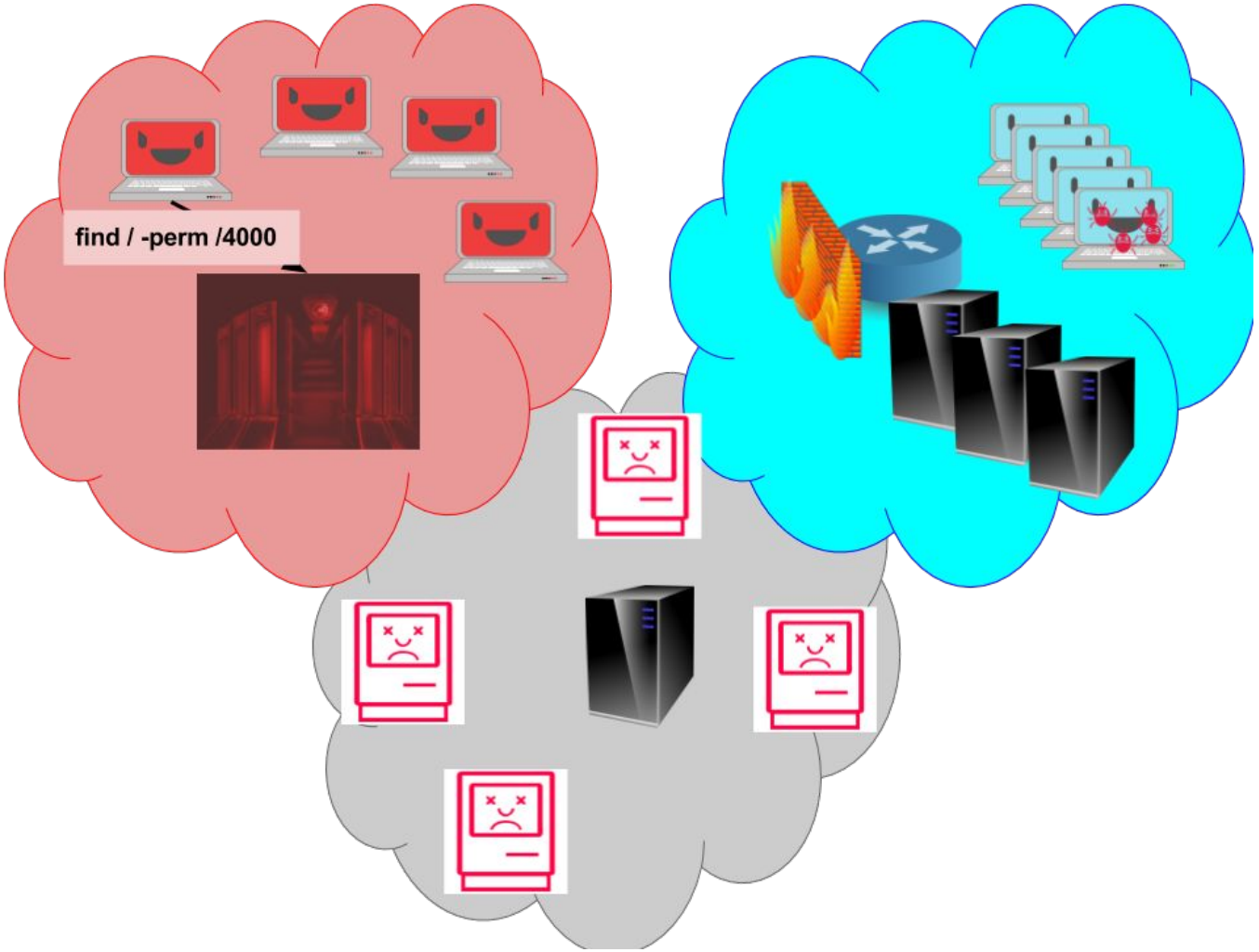
- Understand how the threat operates
- Analyze how to distinguish it from normal
- Implement detection techniques
- Evaluate and refine detection techniques

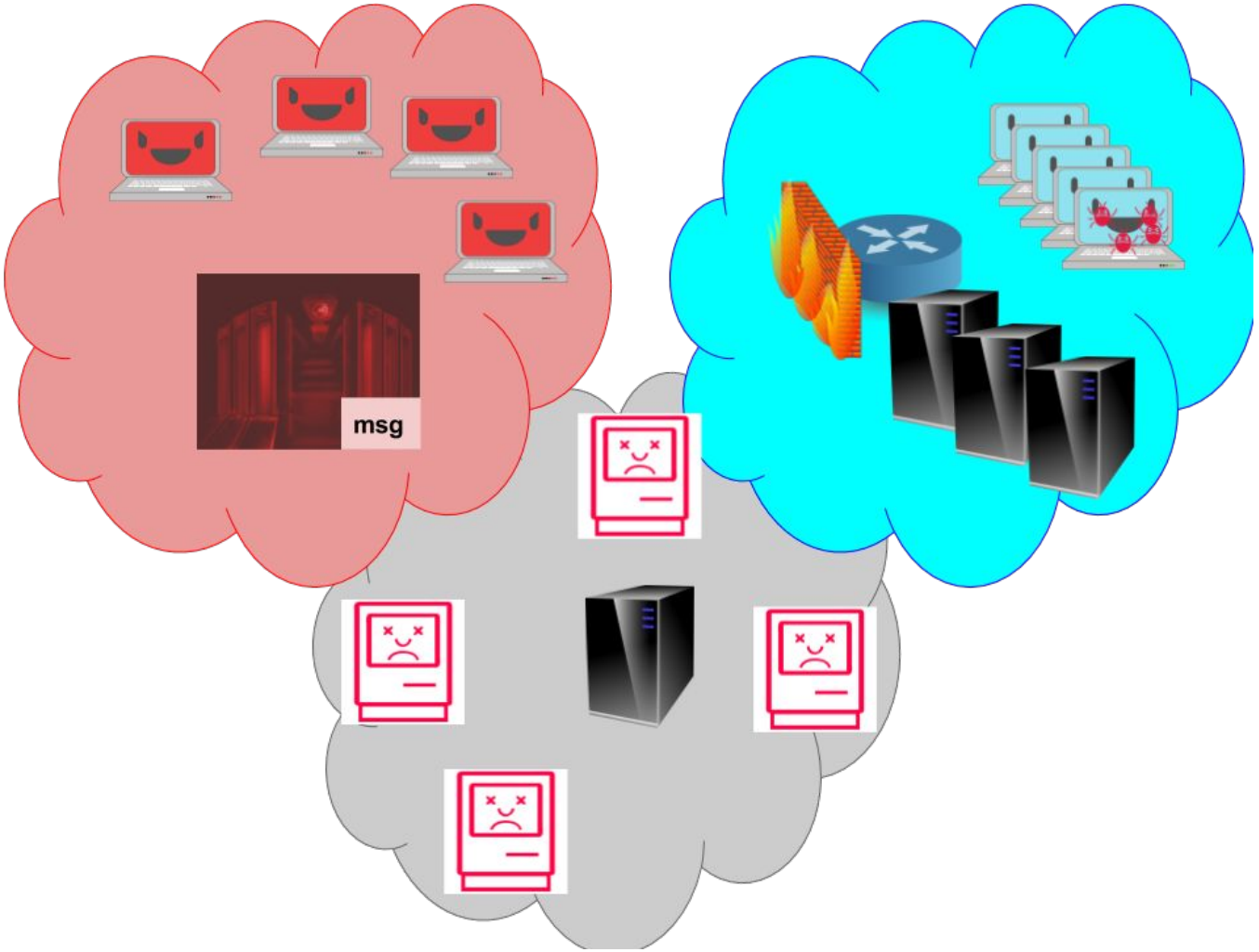
Cobalt Strike

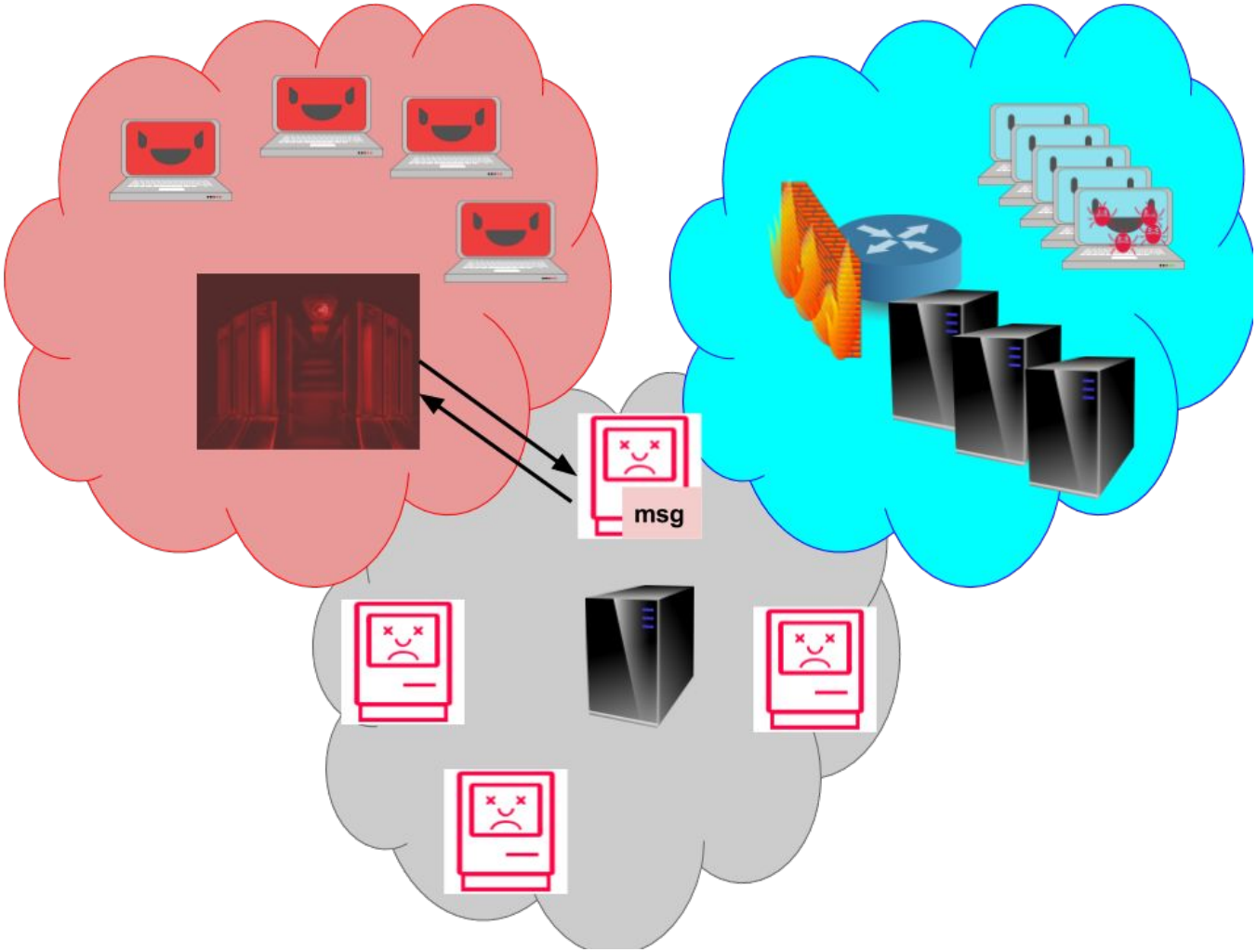
- Commercial penetration testing platform
- Evolved from Armitage
- More than a front-end to Metasploit
  - Enables team offensive operations
  - Has a sophisticated payload delivery mechanism
  - Has a sophisticated callback mechanisms
    - A store-and-forward architecture via “beacons”
    - Beacons for DNS, HTTP, HTTPS, SMB
    - SMB only for inter-beacon communication

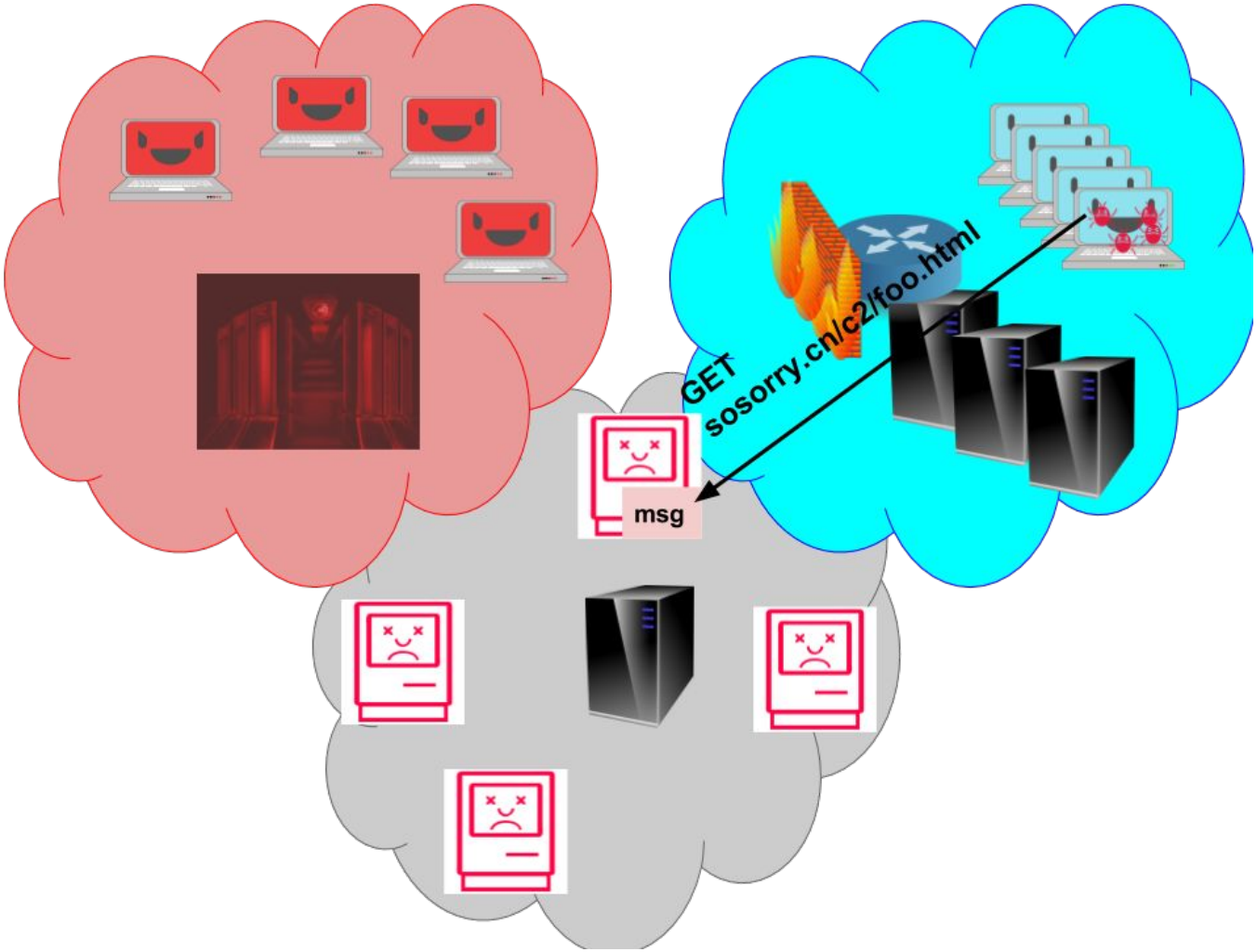
How Cobalt Strike Works

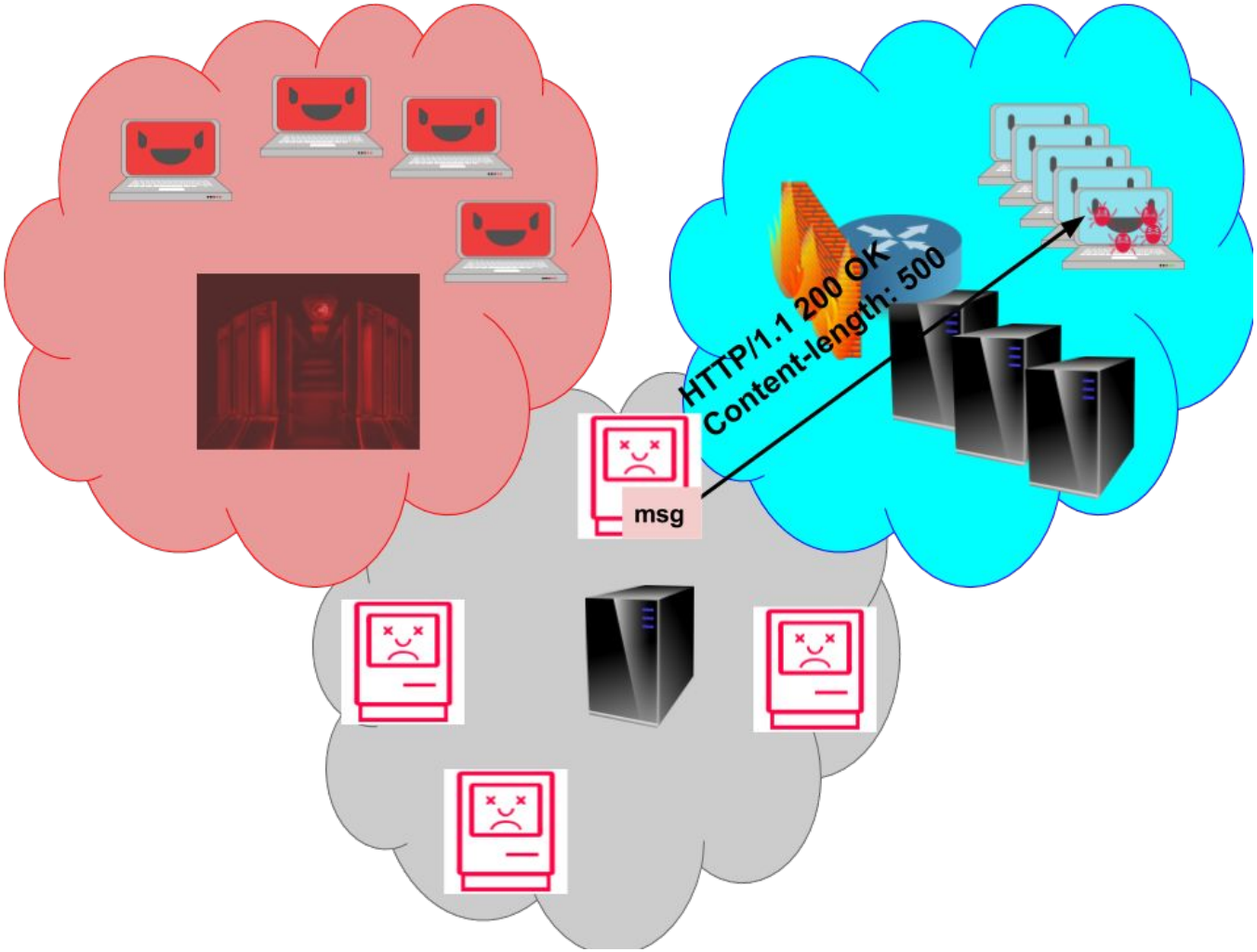


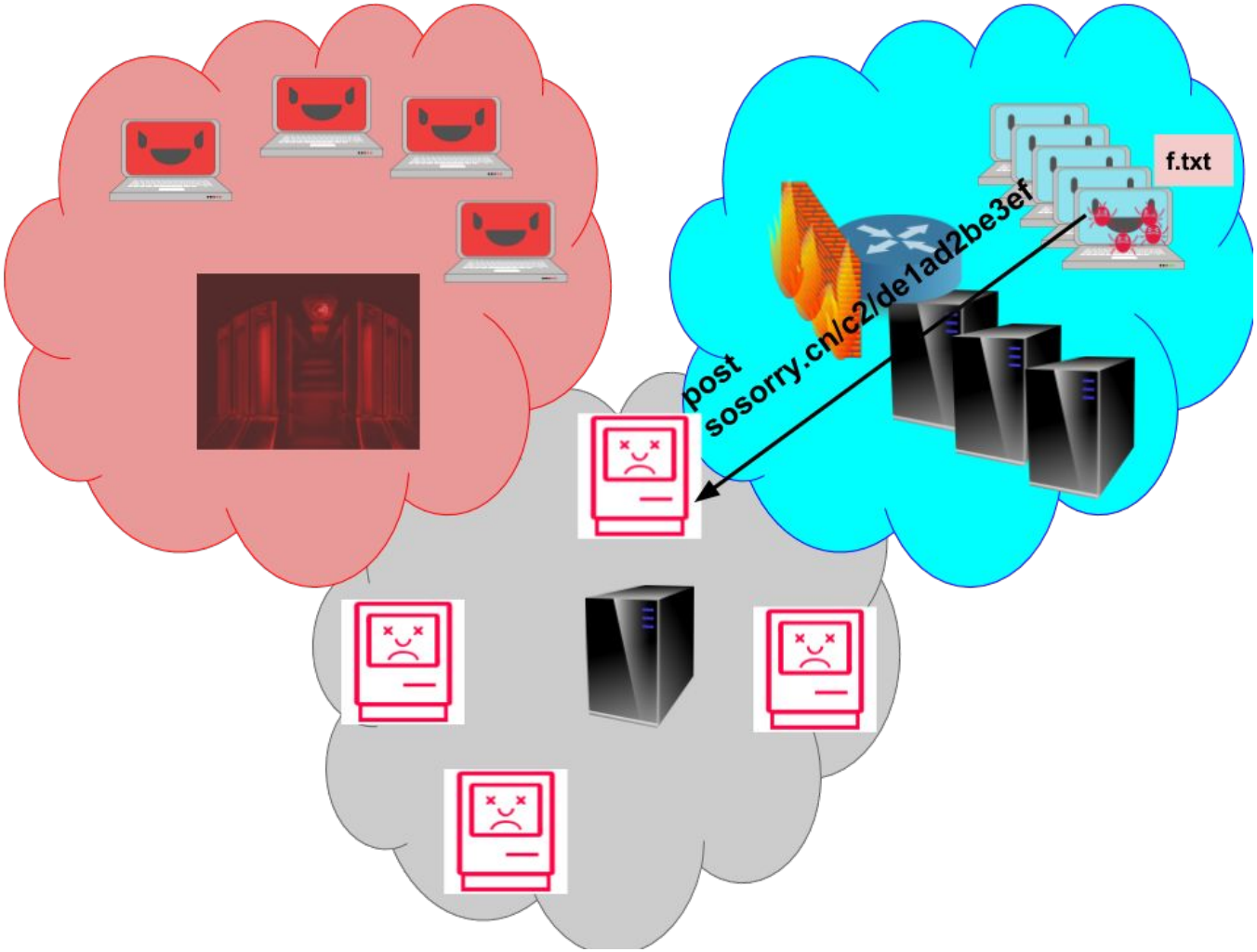

find / -perm /4000

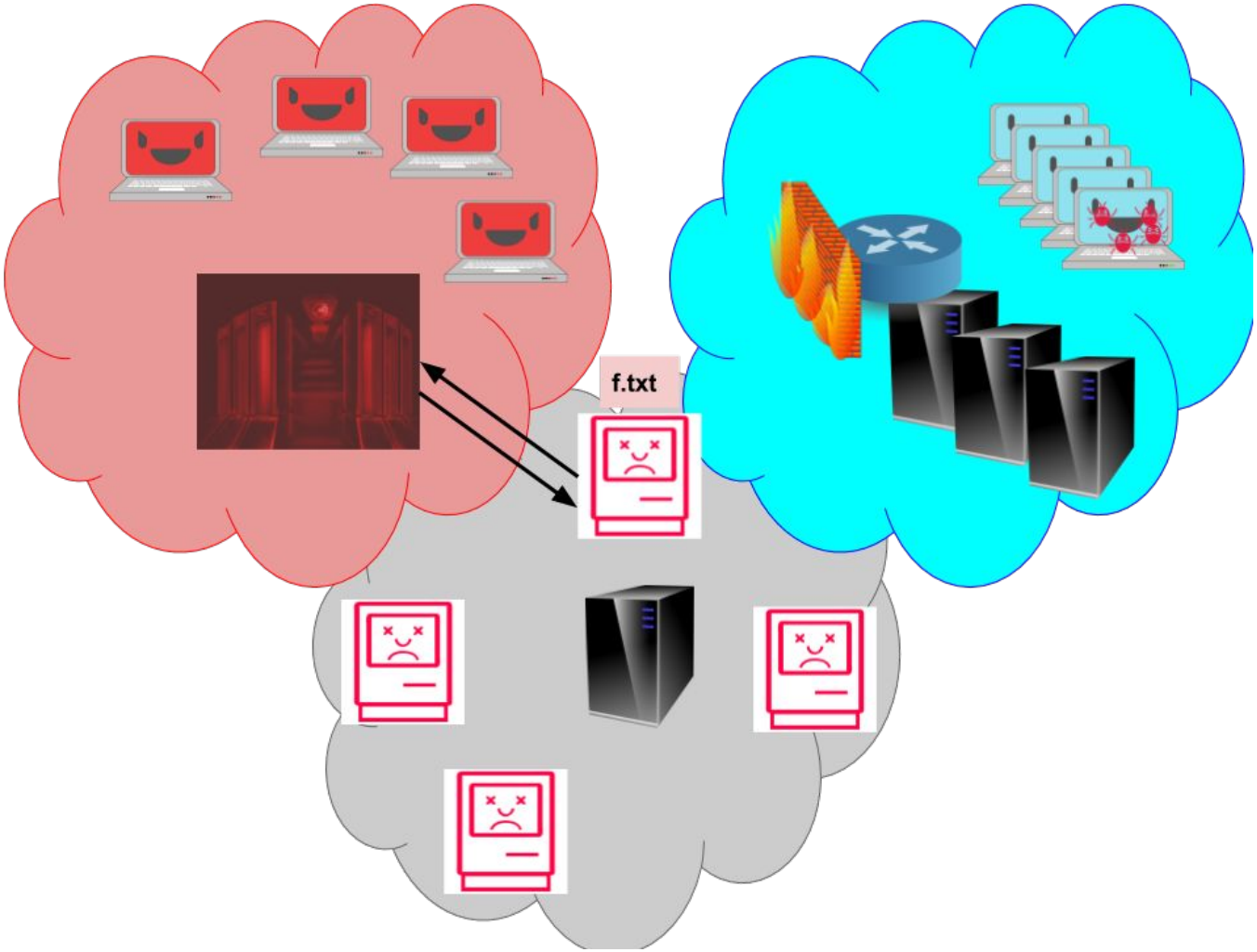

msg

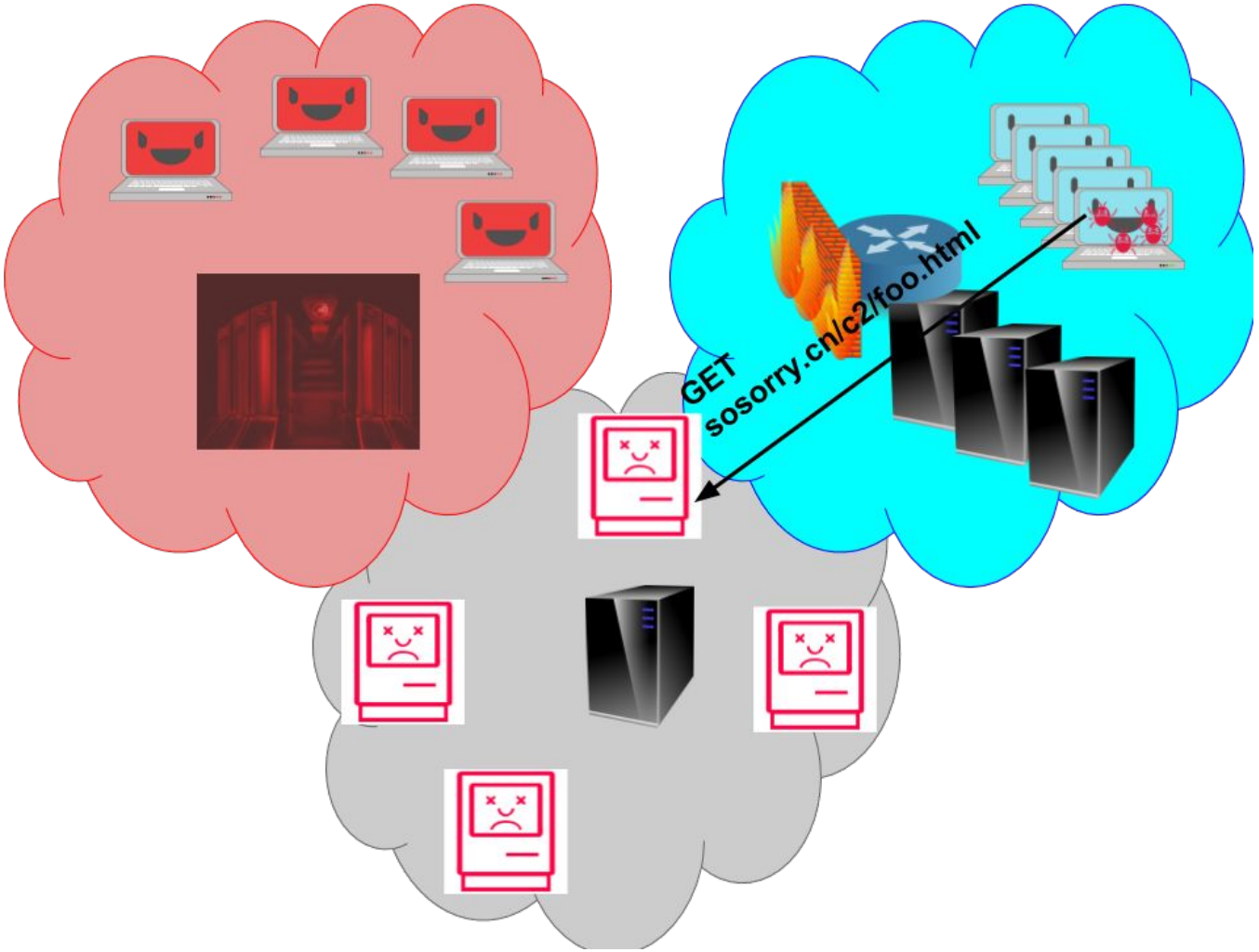

msg

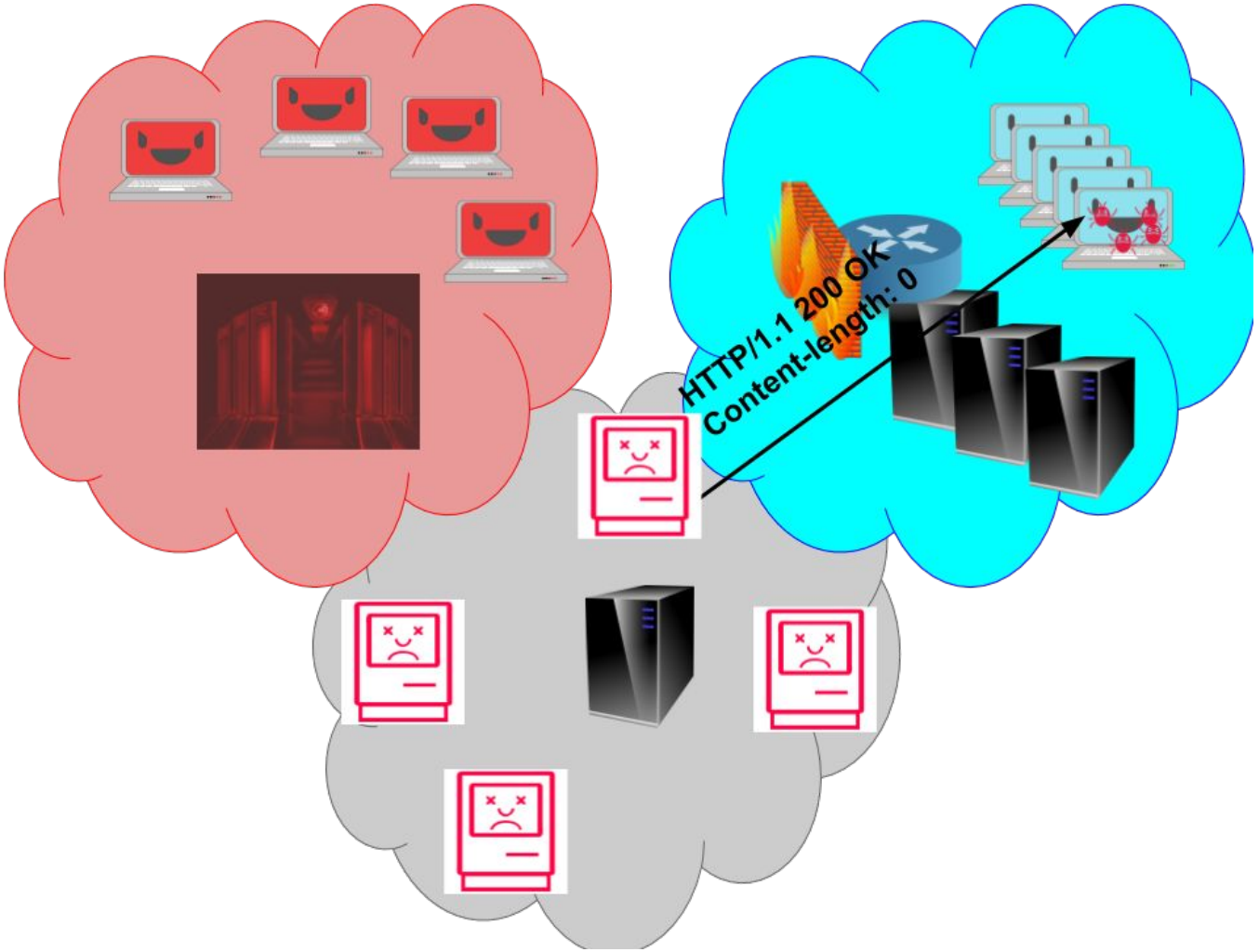

GET
sosorry.cn/c2/foo.html
msg

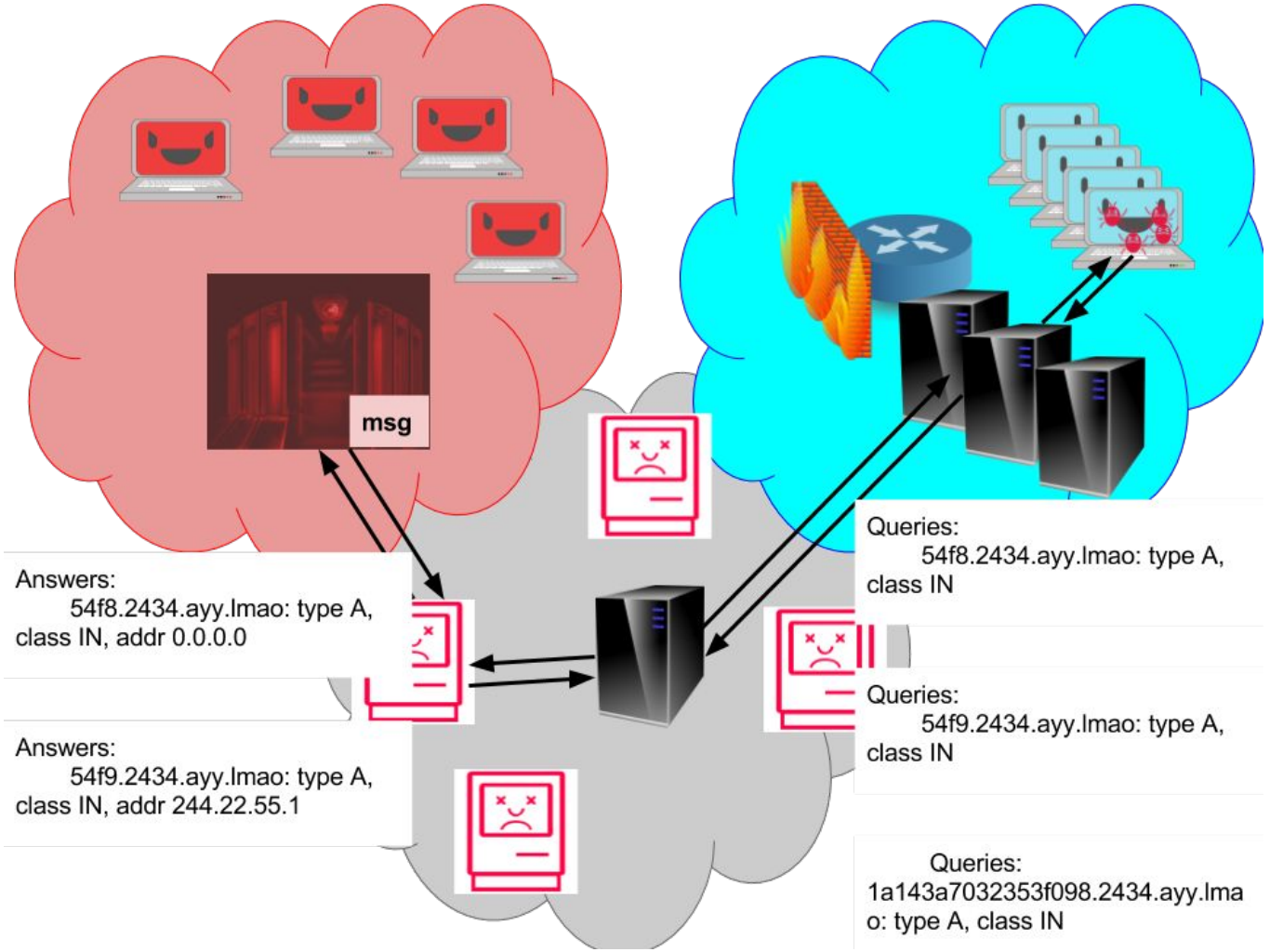

HTTP/1.1 200 OK
Content-length: 500
msg


f.txt
post
sosorry.cn/c2/de1ad2be3ef


f.txt


GET
sosorry.cn/c2/foo.html


HTTP/1.1 200 OK
Content-length: 0


msg
Queries:
54f8.2434.ayy.lmao: type A, class IN
Answers:
54f8.2434.ayy.lmao: type A, class IN, addr 0.0.0.0
Queries:
54f9.2434.ayy.lmao: type A, class IN
Answers:
54f9.2434.ayy.lmao: type A, class IN, addr 244.22.55.1
Queries:
1a143a7032353f098.2434.ayy.lmao: type A, class IN

Traffic Analysis

- Stateless
  - HTTP
    - User agent string outlier detection
    - High entropy payloads
  - DNS
    - Nonce domains / high entropy subdomains
    - Reserved IP use in answers
- Stateful
  - HTTP
    - Post/Get ratios
  - DNS
    - Excessive number of classful networks mappings to single base domain

Traffic Analysis

- Stateless
  - HTTP
    - User agent string outlier detection
    - ~~High entropy payloads~~
  - DNS
    - Nonce domains / ~~high entropy subdomains~~
    - Reserved IP use in answers
- Stateful
  - HTTP
    - Post/Get ratios
  - DNS
    - Excessive number of classful networks mappings to single base domain

broFreq isolated_http.log > isolated_http.freq; cat isolated_http.freq | bro-cut user_agent | uniq

https://github.com/spitfire55/MegaDev

Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; ASU2JS): 3, stdDevs: -0.1200890695172343
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MDDRJS): 4, stdDevs: -0.11990512833039078
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2; .NET4.0C; .NET4.0E): 4, stdDevs: -0.11990512833039078
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64; Trident/6.0; Touch): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MATP; MATP): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUSMSNIP): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; XBLWP7; ZuneWP7): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; Xbox): 4, stdDevs: -0.11990512833039078
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30): 4, stdDevs: -0.11990512833039078
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1): 4, stdDevs: -0.11990512833039078
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; FunWebProducts): 4, stdDevs: -0.11990512833039078
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; NP06): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;NLNL): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; MDDCJS): 5, stdDevs: -0.11972118714354728
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.3; .NET CLR 2.0.50727): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; MAM2): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0; LG; LG-E906): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; WOW64; Trident/5.0): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; NP06): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; NP07; NP07): 5, stdDevs: -0.11972118714354728
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BOIE9;ENUS): 6, stdDevs: -0.11953724595670376
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; MALNJS): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Win64; x64; Trident/6.0; ASU2JS): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUSMSE): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0; BO1IE8_v1;ENUS): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; MALC): 6, stdDevs: -0.11953724595670376
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0): 6, stdDevs: -0.11953724595670376
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.1): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0; MASP): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; BOIE9;ENUS): 6, stdDevs: -0.11953724595670376
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0): 6, stdDevs: -0.11953724595670376
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MANM): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser): 7, stdDevs: -0.11935330476986025
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.4; InfoPath.2): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0): 8, stdDevs: -0.11916936358301673
Microsoft-CryptoAPI/6.3: 8, stdDevs: -0.11916936358301673
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0): 8, stdDevs: -0.11916936358301673
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322): 8, stdDevs: -0.11916936358301673
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;ENUSMSE): 10, stdDevs: -0.1188014812093297
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0): 10, stdDevs: -0.1188014812093297
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0): 10, stdDevs: -0.1188014812093297
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0): 16, stdDevs: -0.11769783408826864
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; QQDownload 733; .NET CLR 2.0.50727): 71, stdDevs: -0.10758106881187547
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0: 96, stdDevs: -0.10298253914078767
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0): 139, stdDevs: -0.09507306810651665
Mozilla/5.0: 675, stdDevs: 0.0035194080416058645
-: 7732, stdDevs: 1.3015923635962712
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko: 11451, stdDevs: 1.9856696374672926
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1): 58115, stdDevs: 10.569101180332943
Average: 655.8666666666667
StdDev: 5436.520320219252
-

```
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; Trident/6.0): 6, stdDevs: -0.11953724595670376
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MANM): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/5.0): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; Avant Browser): 7, stdDevs: -0.11935330476986025
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.4; InfoPath.2): 7, stdDevs: -0.11935330476986025
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0): 8, stdDevs: -0.11916936358301673
Microsoft-CryptoAPI/6.3: 8, stdDevs: -0.11916936358301673
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0): 8, stdDevs: -0.11916936358301673
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322): 8, stdDevs: -0.11916936358301673
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;ENUSMSE): 10, stdDevs: -0.1188014812093297
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0): 10, stdDevs: -0.1188014812093297
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0): 10, stdDevs: -0.1188014812093297
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0): 16, stdDevs: -0.11769783408826864
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; QQDownload 733; .NET CLR 2.0.50727): 71, stdDevs: -0.10758106881187547
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0: 96, stdDevs: -0.10298253914078767
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0): 139, stdDevs: -0.09507306810651665
Mozilla/5.0: 675, stdDevs: 0.0035194080416058645
-: 7732, stdDevs: 1.3015923635962712
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko: 11451, stdDevs: 1.9856696374672926
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1): 58115, stdDevs: 10.569101180332943
Average: 655.8666666666667
StdDev: 5436.520320219252
-
```

Doesn’t seem legit….

- cat isolated_http.log | bro-cut host | sort | uniq | wc -l
  - 15177
- cat isolated_http.log | bro-cut host user_agent | grep "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)" | uniq
    - sosorry.ca Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- cat isolated_http.log | bro-cut host method > hostVmethod.txt; getPostCompare hostVmethod.txt

https://github.com/spitfire55/MegaDev

cat isolated_http.log | bro-cut host method > hostVmethod.txt; getPostCompare hostVmethod.txt

Hostname	Number of Gets	Number of Posts	Get/Post Ratio
rubberneck.hq.bluenet	2057.0	3705.0	0.5552
...			
www.mtg.com	51.0	49.0	1.041
10.2.109.174	40.0	8.0	5.0
hammer.com	40.0	8.0	5.0
sosorry.ca	57792.0	323.0	178.92

domainParser

- Takes in a listing of domain names to frequencies and parses them into useful formats for analysis
- A Trie based data structure
- 3 modes
  - “tree” for
    - A hierarchical representation
    - Can set desired branch depth
  - “text” output
    - Tabular listing of statistics for each domain name
    - Can set the desired level of subdomains to analyze, ie, www.foo.bar has three levels
    - Can set a minimum threshold of child subdomains for a domain
- https://github.com/spitfire55/MegaDev

domainParser cdx_query_freq.dns --text 3 50 > text_to_display_textout_3_50.txt

```
ntp.org.localdomain. Num of instances where fqn 0 Num child domains: 1 Tot instances: 4517
mozilla.net.localdomain. Num of instances where fqn 0 Num child domains: 1 Tot instances: 53300
60.0/24.localdomain. Num of instances where fqn 0 Num child domains: 1 Tot instances: 152
smartscreen.microsoft.com. Num of instances where fqn 0 Num child domains: 1 Tot instances: 245
cms.msn.com. Num of instances where fqn 0 Num child domains: 1 Tot instances: 63
pool.ntp.org. Num of instances where fqn 499 Num child domains: 1 Tot instances: 27327
_sites.usmma.bluenet. Num of instances where fqn 0 Num child domains: 1 Tot instances: 66
_sites.usma.bluenet. Num of instances where fqn 0 Num child domains: 1 Tot instances: 715
be.usma.bluenet. Num of instances where fqn 0 Num child domains: 1 Tot instances: 140
ca.usma.bluenet. Num of instances where fqn 0 Num child domains: 1 Tot instances: 60
localdomain.eecs.net. Num of instances where fqn 0 Num child domains: 1 Tot instances: 1688
naples.navy.mil. Num of instances where fqn 0 Num child domains: 1 Tot instances: 6503
default-first-site-name._sites.dc1. Num of instances where fqn 0 Num child domains: 1 Tot instances: 633
mozilla.com.localdomain. Num of instances where fqn 0 Num child domains: 2 Tot instances: 1929
appex.bing.com. Num of instances where fqn 0 Num child domains: 2 Tot instances: 2014
forestdnszones.usma.bluenet. Num of instances where fqn 0 Num child domains: 2 Tot instances: 355
dc1.usma.bluenet. Num of instances where fqn 180647 Num child domains: 2 Tot instances: 3883
domaindnszones.usma.bluenet. Num of instances where fqn 0 Num child domains: 2 Tot instances: 523
org.eecs.net. Num of instances where fqn 0 Num child domains: 2 Tot instances: 413
bluenet.eecs.net. Num of instances where fqn 0 Num child domains: 2 Tot instances: 13163
us.leaseweb.net. Num of instances where fqn 0 Num child domains: 2 Tot instances: 249
f.ip6.arpa. Num of instances where fqn 0 Num child domains: 3 Tot instances: 80507
data.microsoft.com. Num of instances where fqn 0 Num child domains: 3 Tot instances: 3144
_msdcs.cdx.bluenet. Num of instances where fqn 0 Num child domains: 3 Tot instances: 3798
10.in-addr.arpa. Num of instances where fqn 0 Num child domains: 4 Tot instances: 61243
_msdcs.usma.bluenet. Num of instances where fqn 0 Num child domains: 4 Tot instances: 3551
ubuntu.com.localdomain. Num of instances where fqn 0 Num child domains: 6 Tot instances: 77
mozilla.org.localdomain. Num of instances where fqn 0 Num child domains: 6 Tot instances: 3558
bluenet.usma.bluenet. Num of instances where fqn 0 Num child domains: 11 Tot instances: 80972
mil.usma.bluenet. Num of instances where fqn 0 Num child domains: 12 Tot instances: 722
27628.dnd.net. Num of instances where fqn 8 Num child domains: 17 Tot instances: 136
5957.dnd.net. Num of instances where fqn 8 Num child domains: 17 Tot instances: 148
gov.usma.bluenet. Num of instances where fqn 0 Num child domains: 19 Tot instances: 119
net.usma.bluenet. Num of instances where fqn 0 Num child domains: 24 Tot instances: 10980
org.usma.bluenet. Num of instances where fqn 0 Num child domains: 34 Tot instances: 11839
edu.usma.bluenet. Num of instances where fqn 0 Num child domains: 38 Tot instances: 12788
nmkrtsptaab.cyberknights.com. Num of instances where fqn 0 Num child domains: 53 Tot instances: 53
nmkrtsptaab.coffeebreath.net. Num of instances where fqn 0 Num child domains: 72 Tot instances: 117
com.usma.bluenet. Num of instances where fqn 0 Num child domains: 162 Tot instances: 12318
nmkrtsptaab.cyberrenegades.com. Num of instances where fqn 0 Num child domains: 264 Tot instances: 499
31727.scoreboard.cdx. Num of instances where fqn 547 Num child domains: 1029 Tot instances: 2360
4207.scoreboard.cdx. Num of instances where fqn 690 Num child domains: 1193 Tot instances: 2601
11240.scoreboard.cdx. Num of instances where fqn 154 Num child domains: 1245 Tot instances: 3796
7071.verizon.net. Num of instances where fqn 18 Num child domains: 1479 Tot instances: 2972
20776.lenovo.com. Num of instances where fqn 15 Num child domains: 71508 Tot instances: 181407
2722.lenovo.com. Num of instances where fqn 16 Num child domains: 71529 Tot instances: 145144
nmkrtsptaab.sharklazers.net. Num of instances where fqn 0 Num child domains: 309182 Tot instances: 309214
nmkrtsptaab.cybermugging.net. Num of instances where fqn 0 Num child domains: 376105 Tot instances: 376372
```

telemetry.microsoft.com. Num of instances where fqn 0 Num child domains: 4 Tot instances: 4
_msdcs.usma.bluenet. Num of instances where fqn 0 Num child domains: 4 Tot instances: 3551
tolfesptaab.cybermugging.net. Num of instances where fqn 0 Num child domains: 4 Tot instances: 4
centos.org.localdomain. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
hq.bluenet.localdomain. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
tolfesptaab.cyberknights.com. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
_tcp.usma.bluenet. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
nmkrtsptaab.telemetry.net. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
g.akamaitech.net. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
tolfesptaab.oz.net. Num of instances where fqn 0 Num child domains: 5 Tot instances: 11
ubuntu.com.localdomain. Num of instances where fqn 0 Num child domains: 6 Tot instances: 77
mozilla.org.localdomain. Num of instances where fqn 0 Num child domains: 6 Tot instances: 3558
nmkrtsptaab.cyberbattlefield.com. Num of instances where fqn 0 Num child domains: 6 Tot instances: 6
nmkrtsptaab.billfreakinmurray.com. Num of instances where fqn 0 Num child domains: 6 Tot instances: 6
simnet.usma.bluenet. Num of instances where fqn 0 Num child domains: 6 Tot instances: 6
usma.bluenet.localdomain. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
tolfesptaab.billfreakinmurray.com. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
nmkrtsptaab.theglider.net. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
nmkrtsptaab.cybershells.net. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
nmkrtsptaab.meeshell.com. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
tolfesptaab.cybercelebrations.com. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
nmkrtsptaab.dhclienteth0.com. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
g.akamai.net. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
google.com.localdomain. Num of instances where fqn 32 Num child domains: 9 Tot instances: 9
nmkrtsptaab.oz.net. Num of instances where fqn 0 Num child domains: 9 Tot instances: 9
tolfesptaab.theglider.net. Num of instances where fqn 0 Num child domains: 10 Tot instances: 10
bluenet.usma.bluenet. Num of instances where fqn 0 Num child domains: 11 Tot instances: 80972
nmkrtsptaab.cybercelebrations.com. Num of instances where fqn 0 Num child domains: 12 Tot instances: 18
sig-dc1.usma.bluenet. Num of instances where fqn 0 Num child domains: 12 Tot instances: 12
mil.usma.bluenet. Num of instances where fqn 0 Num child domains: 12 Tot instances: 722
tolfesptaab.cyberrenegades.com. Num of instances where fqn 0 Num child domains: 15 Tot instances: 15
nmkrtsptaab.thisisntalonghaul.net. Num of instances where fqn 0 Num child domains: 16 Tot instances: 21
nmkrtsptaab.thebatwing.com. Num of instances where fqn 0 Num child domains: 17 Tot instances: 17
20776.halo.com. Num of instances where fqn 8 Num child domains: 17 Tot instances: 34
2722.usafa.edu. Num of instances where fqn 14 Num child domains: 17 Tot instances: 34
27628.dnd.net. Num of instances where fqn 8 Num child domains: 17 Tot instances: 136
5957.dnd.net. Num of instances where fqn 8 Num child domains: 17 Tot instances: 148
7071.ps3.net. Num of instances where fqn 49 Num child domains: 18 Tot instances: 35
nmkrtsptaab.globogym.net. Num of instances where fqn 0 Num child domains: 18 Tot instances: 18
gov.usma.bluenet. Num of instances where fqn 0 Num child domains: 19 Tot instances: 119
nmkrtsptaab.lazerblazer.com. Num of instances where fqn 0 Num child domains: 23 Tot instances: 32
net.usma.bluenet. Num of instances where fqn 0 Num child domains: 24 Tot instances: 10980
nmkrtsptaab.verizone.com. Num of instances where fqn 0 Num child domains: 29 Tot instances: 29
org.usma.bluenet. Num of instances where fqn 0 Num child domains: 34 Tot instances: 11839
nmkrtsptaab.zebracakes.com. Num of instances where fqn 0 Num child domains: 35 Tot instances: 35
edu.usma.bluenet. Num of instances where fqn 0 Num child domains: 38 Tot instances: 12788
nmkrtsptaab.cyberknights.com. Num of instances where fqn 0 Num child domains: 53 Tot instances: 53
nmkrtsptaab.coffeebreath.net. Num of instances where fqn 0 Num child domains: 72 Tot instances: 117
com.usma.bluenet. Num of instances where fqn 0 Num child domains: 162 Tot instances: 12318
nmkrtsptaab.cyberrenegades.com. Num of instances where fqn 0 Num child domains: 264 Tot instances: 499
31727.scoreboard.cdx. Num of instances where fqn 547 Num child domains: 1029 Tot instances: 2360
4207.scoreboard.cdx. Num of instances where fqn 690 Num child domains: 1193 Tot instances: 2601
11240.scoreboard.cdx. Num of instances where fqn 154 Num child domains: 1245 Tot instances: 3796
7071.verizon.net. Num of instances where fqn 18 Num child domains: 1479 Tot instances: 2972
20776.lenovo.com. Num of instances where fqn 15 Num child domains: 71508 Tot instances: 181407
2722.lenovo.com. Num of instances where fqn 16 Num child domains: 71529 Tot instances: 145144
nmkrtsptaab.sharklazers.net. Num of instances where fqn 0 Num child domains: 309182 Tot instances: 309214
nmkrtsptaab.cybermugging.net. Num of instances where fqn 0 Num child domains: 376105 Tot instances: 376372

nmkrtsptaab.peanutbutterjellytime.net. Num of instances where fqn 0 Num child domains: 1 Tot instances: 1
nmkrtsptaab.eaglesnbeagles.com. Num of instances where fqn 0 Num child domains: 3 Tot instances: 3
nmkrtsptaab.averagejoes.net. Num of instances where fqn 0 Num child domains: 3 Tot instances: 3
nmkrtsptaab.telemetry.net. Num of instances where fqn 0 Num child domains: 5 Tot instances: 5
nmkrtsptaab.cyberbattlefield.com. Num of instances where fqn 0 Num child domains: 6 Tot instances: 6
nmkrtsptaab.billfreakinmurray.com. Num of instances where fqn 0 Num child domains: 6 Tot instances: 6
nmkrtsptaab.theglider.net. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
nmkrtsptaab.cybershells.net. Num of instances where fqn 0 Num child domains: 7 Tot instances: 7
nmkrtsptaab.meeshell.com. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
nmkrtsptaab.dhclienteth0.com. Num of instances where fqn 0 Num child domains: 8 Tot instances: 8
nmkrtsptaab.oz.net. Num of instances where fqn 0 Num child domains: 9 Tot instances: 9
nmkrtsptaab.cybercelebrations.com. Num of instances where fqn 0 Num child domains: 12 Tot instances: 18
nmkrtsptaab.thisisntalonghaul.net. Num of instances where fqn 0 Num child domains: 16 Tot instances: 21
nmkrtsptaab.thebatwing.com. Num of instances where fqn 0 Num child domains: 17 Tot instances: 17
nmkrtsptaab.globogym.net. Num of instances where fqn 0 Num child domains: 18 Tot instances: 18
nmkrtsptaab.lazerblazer.com. Num of instances where fqn 0 Num child domains: 23 Tot instances: 32
nmkrtsptaab.verizone.com. Num of instances where fqn 0 Num child domains: 29 Tot instances: 29
nmkrtsptaab.zebracakes.com. Num of instances where fqn 0 Num child domains: 35 Tot instances: 35
nmkrtsptaab.cyberknights.com. Num of instances where fqn 0 Num child domains: 53 Tot instances: 53
nmkrtsptaab.coffeebreath.net. Num of instances where fqn 0 Num child domains: 72 Tot instances: 117
nmkrtsptaab.cyberrenegades.com. Num of instances where fqn 0 Num child domains: 264 Tot instances: 499
nmkrtsptaab.sharklazers.net. Num of instances where fqn 0 Num child domains: 309182 Tot instances: 309214
nmkrtsptaab.cybermugging.net. Num of instances where fqn 0 Num child domains: 376105 Tot instances: 376372

Doesn’t seem legit...

```
                |___self-repair count: 314
                |___addons count: 482
                |___telemetry count: 3072
        |___w3 count: 24
                |___validator count: 24
|___com count: 254483
        |___usma count: 12
                |___www count: 12
        |___nnn count: 2
        |___radioshack count: 6
                |___www count: 6
        |___googlesyndication count: 4
                |___pagead2 count: 4
        |___googleapis count: 551
                |___fonts count: 444
                |___ajax count: 107
        |___phpbb count: 3
                |___www count: 3
        |___gravatar count: 3070
                |___0 count: 3070
        |___starwars count: 2
                |___www count: 2
        |___google count: 734
                |___docs count: 12
                |___safebrowsing count: 658
                |___groups count: 8
                |___labs count: 8
                |___picasaweb count: 8
                |___finance count: 8
                |___books count: 12
                |___blogsearch count: 12
                |___scholar count: 8
        |___store count: 6
                |___www count: 6
        |___mtg count: 4
                |___www count: 4
        |___mlg count: 2
                |___www count: 2
        |___mozillamessaging count: 112
                |___live count: 112
        |___faceb00k count: 4
                |___www count: 4
        |___speedtest count: 4
                |___www count: 4
        |___tzulo count: 36
                |___mirror count: 36
        |___ubuntu count: 247999
                |___ntp count: 161859
                |___productsearch count: 74818
                |___security count: 24
                |___start count: 24
                |___daisy count: 11202
                |___archive count: 72
        |___mozilla count: 1929
                |___services count: 1705
                |___data count: 224
        |___rockhall count: 3
                |___www count: 3
|___localdomain count: 25102
        |___localdomain\x0a#localhost count: 25050
```

```
|___cybermugging count: 376434
        |___nmkrtsptaab count: 376426
                |___g3fee52fd count: 1
                |___g29c741d5 count: 1
                |___g77c5a0b1 count: 1
                |___g4cf9e2e1 count: 1
                |___g4272332d count: 1

|___globogym count: 44
        |___nmkrtsptaab count: 40
                |___g58c8632f count: 2
                |___g136651d9 count: 2
                |___g356f72bb count: 2
                |___c3a582ec3 count: 2
                |___g2f0c02a6 count: 2

|___oz count: 34
        |___nmkrtsptaab count: 20
                |___g3333d3f3 count: 1
                |___c72a48756 count: 2
                |___c6b713a34 count: 1
                |___g51b84008 count: 6
                |___g0cfd0199 count: 6

|___sharklazers count: 357641
        |___nmkrtsptaab count: 357637
                |___g7d4c1222 count: 1
                |___g0bb1f501 count: 1
                |___g68720b7d count: 1
                |___g3985091a count: 1
                |___g22f62dd2 count: 2

|___cybershells count: 29
        |___nmkrtsptaab count: 22
                |___c21719fc4 count: 2
                |___c0382993f count: 2
                |___g2fd97367 count: 6
                |___g3ccc4f21 count: 2
                |___g3d4f7731 count: 6

|___peanutbutterjellytime count: 2
        |___nmkrtsptaab count: 2
                |___c46129961 count: 2
|___averagejokes count: 2
        |___www count: 2
|___revsci count: 166
        |___js count: 108

                |___g4d5be2e5 count: 2
        |___nmkrtsptaab count: 13
                |___g4508c62c count: 1
                |___c25e28868 count: 2
                |___g4a451d10 count: 1
                |___c5d7cdbfe count: 1
                |___g71a28a3d count: 1

|___thisisntalonghaul count: 40
        |___nmkrtsptaab count: 36
                |___g589ff0cf count: 2
                |___g584e21f4 count: 2
```

Evaluation--*CDX 2017*

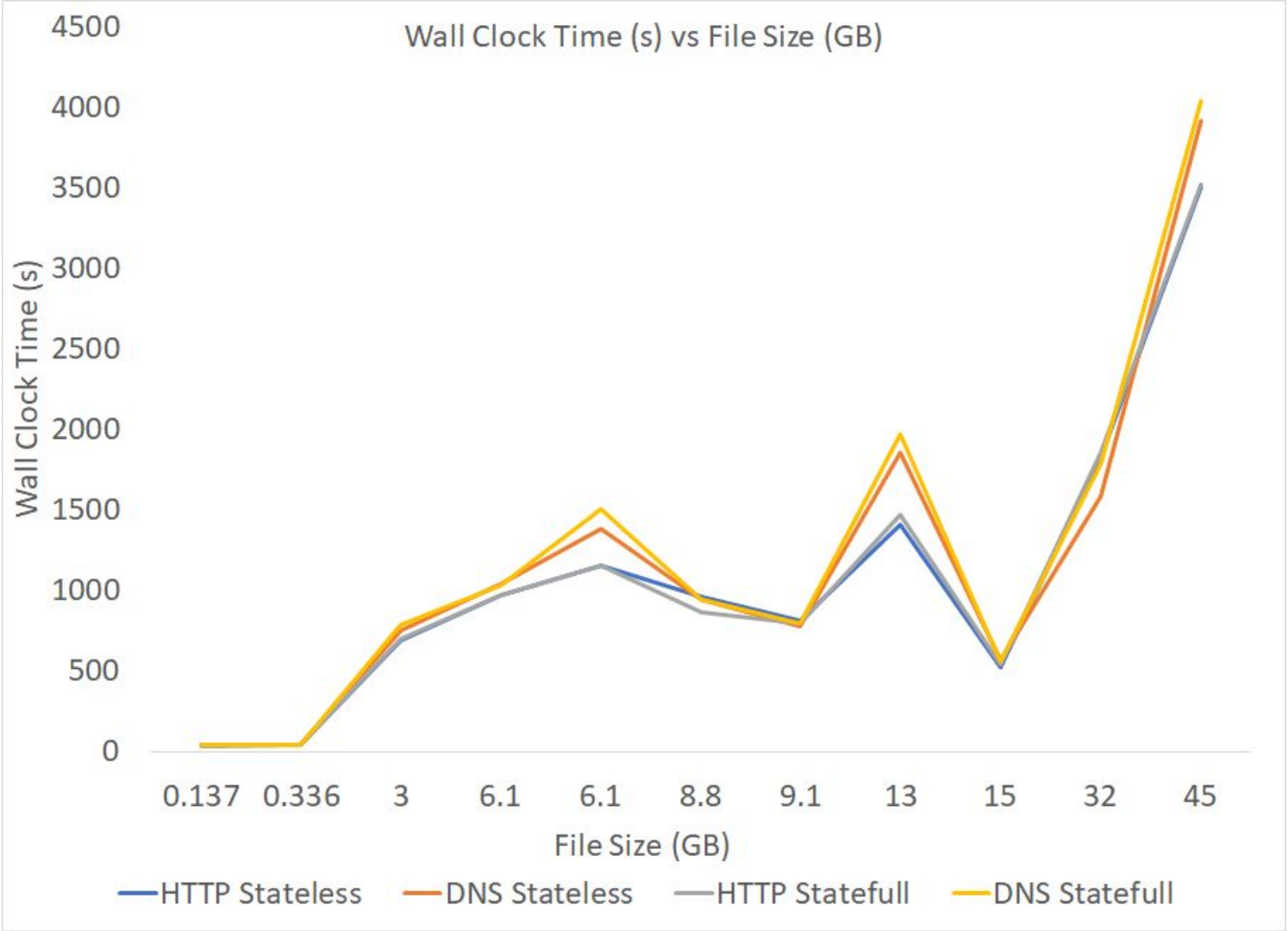
- Part of larger defense-in-depth strategy
  - Elasticsearch-Logstash-Kibana (ELK) SIEM
    - Filebeat ingest from DMZ, firewall and Linux clients
    - Winbeat ingest from Windows clients
  - Snort IDS
  - Cisco ASA
  - Squid Proxy
  - *VisorFlow*: https://www.flyn.org/projects/VisorFlow/index.html
- Bro server
  - CentOS 7, 12 Core, 20 GB RAM
  - PF_RING, full capture
  - Initially co-located with ELK SIEM
  - Move to be co-located with Snort IDS

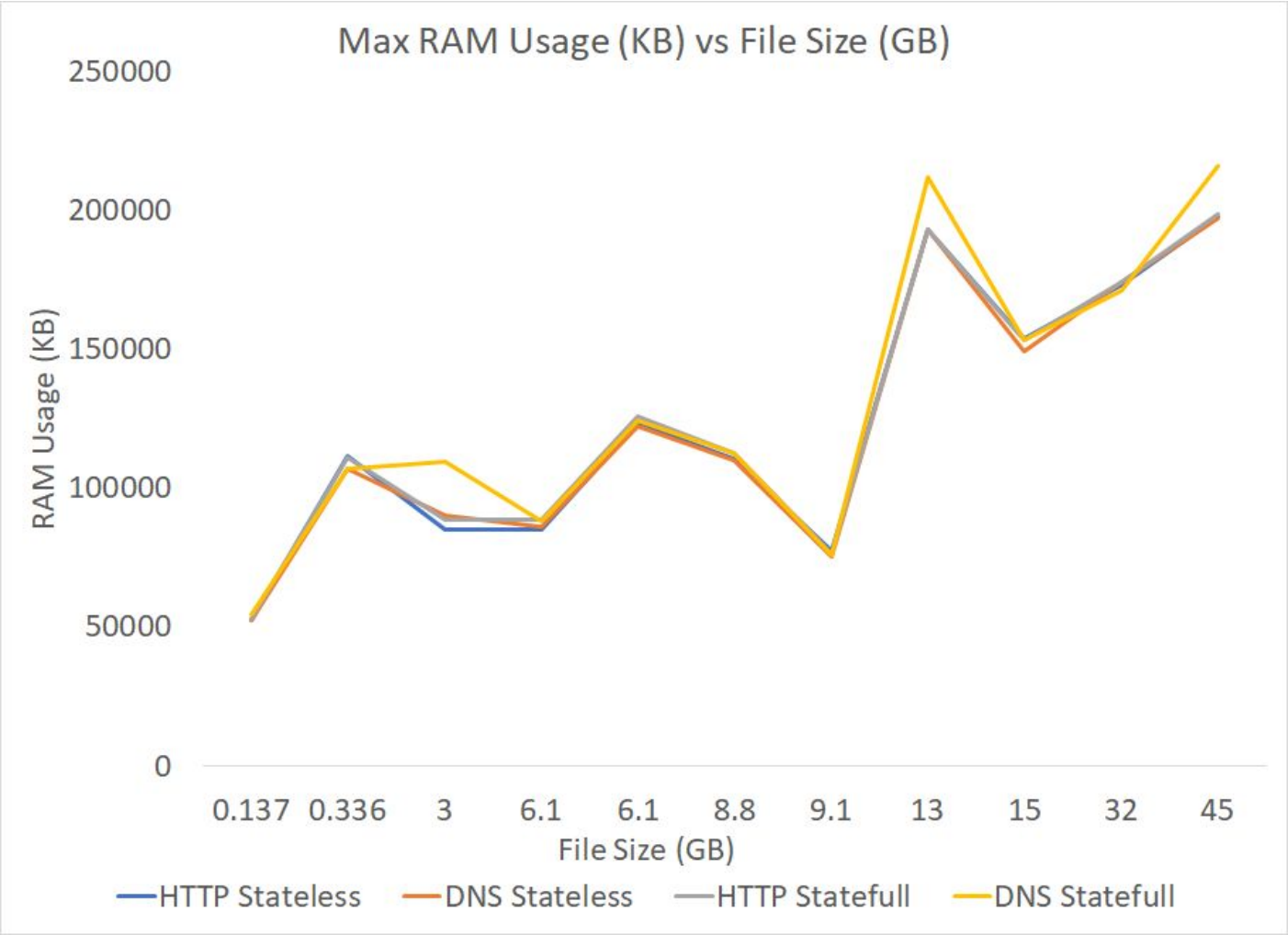
Results

- Reduction of compromises
  - 1035 “token events” during the 2016 CDX
  - 15 “token events” during the 2017 CDX
- Score
  - Highest live competition score
  - 1st Place in confidentiality/integrity category and availability category
  - 8% higher in confidentiality/integrity category than other competitors
- Issues
  - Low number of HTTP/HTTPS events
  - ELK performance
    - High CPU and memory consumption
    - Kibana front-end limitations
  - Not fully leveraging Bro

Evaluation--*Performance testing*

- Xubuntu 14.04 VM
  - Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz
  - 4 Core
  - 9.6 GB RAM
- Data Samples from 2016 and 2017 CDX competition for benchmark purposes


Wall Clock Time (s) vs File Size (GB)
Wall Clock Time (s)
4500
4000
3500
3000
2500
2000
1500
1000
500
0
0.137
0.336
3
6.1
6.1
8.8
9.1
13
15
32
45
File Size (GB)
HTTP Stateless
DNS Stateless
HTTP Statefull
DNS Statefull


Max RAM Usage (KB) vs File Size (GB)
250000
200000
150000
100000
50000
0
RAM Usage (KB)
0.137
0.336
3
6.1
6.1
8.8
9.1
13
15
32
45
File Size (GB)
HTTP Stateless
DNS Stateless
HTTP Statefull
DNS Statefull

Detecting Other Activity--DNSCAT

- DNS-based exfil tool
- Uses MX, CNAME, TXT records
- Enables tunneling
- Much noisier than Cobalt Strike
  - Very long nonce domains
  - Shows up almost immediately in weird.log
- Similar techniques used for Cobalt Strike apply
  - High number of answers to one ***three-level domain name***
  - High entropy subdomains

Take-aways on persistent threats

- Packing exfil data into protocols
  - Trade-off between amount of information transmitted per message and concealment
    - More information, less concealment
    - Less information, more concealment
  - Traffic profile potentially uncharacteristic
- HTTPS is tough
  - SSL with legitimate certificates is hard to detect
  - Must be a deliberate focus
- Importance of understanding “normal”
- Importance of defense-in-depth
- Need to be dynamic/not static

Future Work

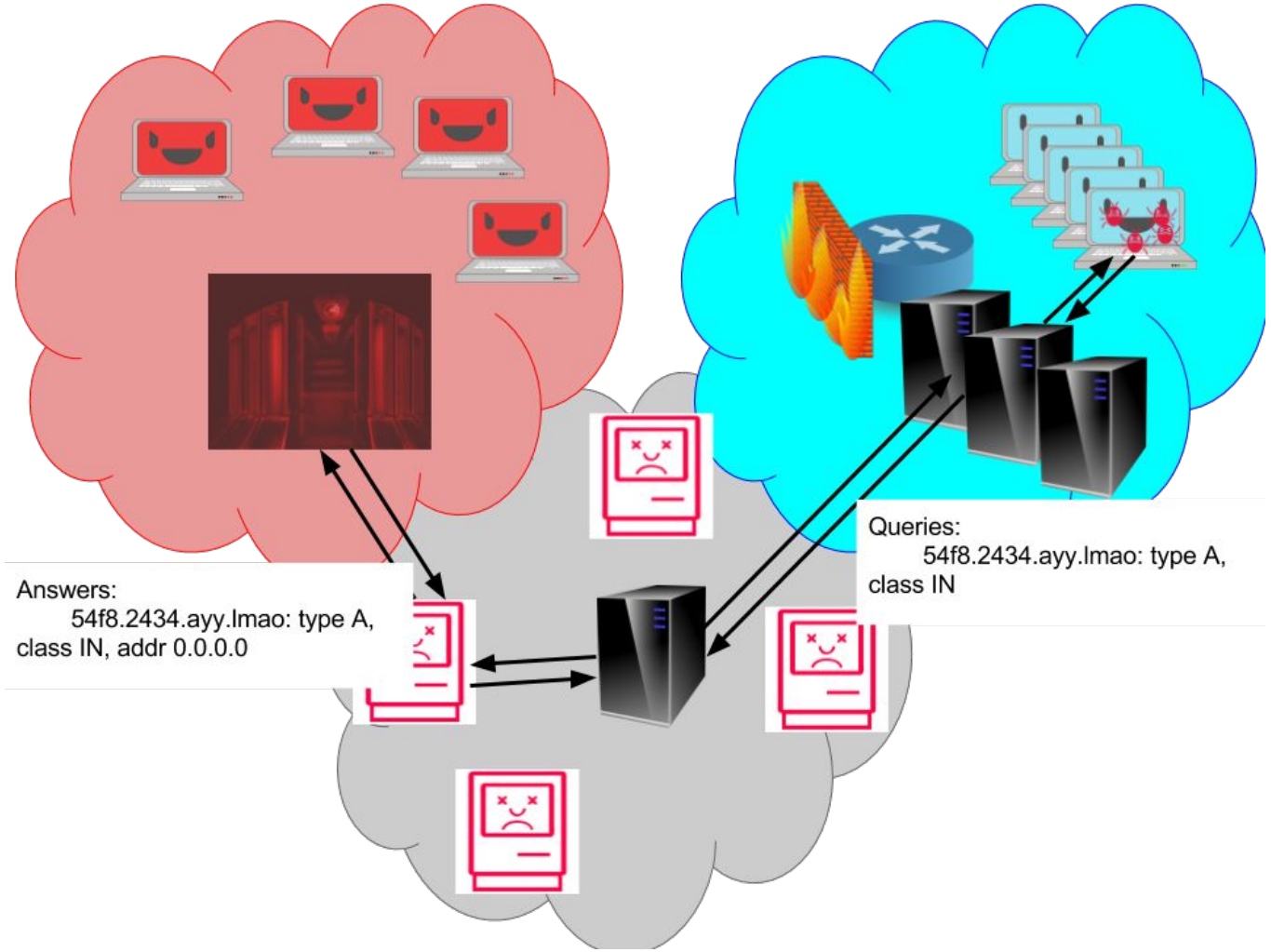
- Continuation of this work
  - Database connections/memory management to scale
  - Other entropy measures for string/domain name characterization
- Other directions
  - Instrumenting more signs of persistence/covert exfil
  - Tool fingerprinting
  - Benchmarking
    - Stateful scripts
    - Performance evaluations for different backend storage solutions
- Potential new features to the Bro framework
  - ssl / x509 anomalies to weird.log
  - Additional data structures

Questions
https://github.com/spitfire55/MegaDev

References

- CrowdStrike. “Adversary Hunting And Incident Response: Network Edition.” BlackHat 2016
- Zeltser, Lenny. “Tunneling Data and Commands Over DNS to Bypass Firewalls.” https://zeltser.com/c2-dns-tunneling/
- Iagox86. “dnscat2.” https://github.com/iagox86/dnscat2
- Mudge, Raphael. *Advanced Threat Tactics for Penetration Testers*. https://www.cobaltstrike.com/training

Backup


Answers:
54f8.2434.ayy.lmao: type A, class IN, addr 0.0.0.0
Queries:
54f8.2434.ayy.lmao: type A, class IN

Implementation

```
}

# DNS Request - Event IDs 40 to 59
# Input: DNS Request information
# Output: Log entries that indicate one (or more) of the following abnormal signatures was found:
#    - High number of subdomains
#    - Hexadecimal subdomain
event dns_request(c: connection, msg:dns_msg, query: string, qtype: count, qclass: count) {
    local event_id = 40;
    local subdomains = split_string(query, /\./);
    local whitelisted = whitelist_domain_check(subdomains);
    local base_domain = get_top_domains(query); #cat_sep(".", "", subdomains[|subdomains|-3], subdomains[|subdomains|-2], subdomains[|subdomains|-1]);
    # EVENT ID 45 - HIGH NUMBER OF SUBDOMAINS
    print fmt("%s", subdomains);
    if ((|subdomains| > 4) && ! whitelisted) {
        # Reconstructs the subdomains to remove subdomains (i.e. foo.bar.xyz.cnn.org -> xyz.cnn.org )
        push_ab_dns_log(c, event_id+5, "High Number of Subdomains", query+"==>"+base_domain);
    }
    # EVENT ID 50 - HEXADECIMAL SUBDOMAIN
    if (check_hex_only_subdomain(subdomains) && ! whitelisted) {
        push_ab_dns_log(c, event_id+10, "Hexadecimal Subdomain", query+"==>"+base_domain);
        }
}

# EVENT ID 55 - A RECORD REPLY RESERVED IP ADDRESS
# Detects whether the IPv4 address is in reserved subnet
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr) {
    if(get_class_network(a) in set_reserved_ipv4_subnets) push_ab_dns_log(c,55,"A Record Reply Reserved IP Address",fmt("%s",a));
    local top = get_top_domains(ans$query);
    if(top in dn_record_store){
        local top_set = dn_record_store[top];
        add top_set[a];
        if( |top_set| > 9) push_ab_dns_log(c, 57, fmt("A Record Reply that maps too many (%s) IPs to a subdomain", |top_set|),fmt(top+" ==> %s",a));
        dn_record_store[top]=top_set;
        }
    else{
        dn_record_store[top] = set(a);
    }
}
```

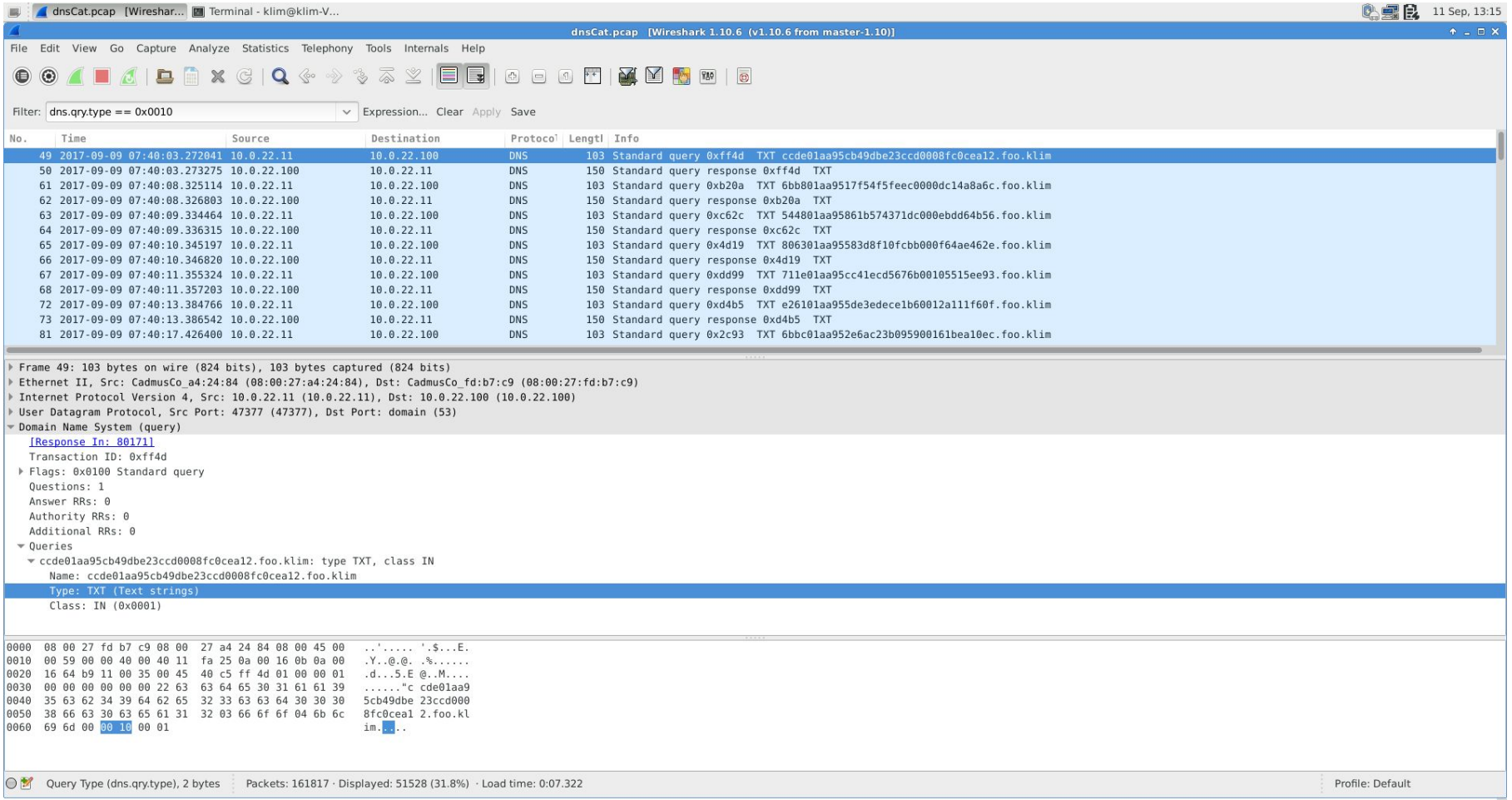
```
        push_ab_dns_log(c, event_id+10, "Hexadecimal Subdomain", query+"==>"+base_domain);
        }
}

# EVENT ID 55 - A RECORD REPLY RESERVED IP ADDRESS
# Detects whether the IPv4 address is in reserved subnet
event dns_A_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr) {
    if(get_class_network(a) in set_reserved_ipv4_subnets) push_ab_dns_log(c,55,"A Record Reply Reserved IP Address",fmt("%s",a));
    local top = get_top_domains(ans$query);
    if(top in dn_record_store){
        local top_set = dn_record_store[top];
        add top_set[a];
        if( |top_set| > 9) push_ab_dns_log(c, 57, fmt("A Record Reply that maps too many (%s) IPs to a subdomain", |top_set|),fmt(top+" ==> %s",a));
        dn_record_store[top]=top_set;
        }
    else{
        dn_record_store[top] = set(a);
    }
}


# EVENT ID 65 - AAAA RECORD REPLY RESERVED IP ADDRESS
# Detects whether the IPv6 address is in reserved subnet
event dns_AAAA_reply(c: connection, msg: dns_msg, ans: dns_answer, a: addr) {
    for (cidr in reserved_ipv6_subnets) {
        if (a in cidr) {
           push_ab_dns_log(c,65,"AAAA Record Reply Reserved IP Address",fmt("%s",a));
        }
    }
    local top = get_top_domains(ans$query);
    if(top in dn_aaaa_record_store){
        local top_set = dn_aaaa_record_store[top];
        add top_set[a];
        if( |top_set| > 9) push_ab_dns_log(c, 67, fmt("AAAA Record Reply that maps too many (%s) IPs to a subdomain", |top_set|),fmt(top+" ==> %s",a));
        dn_aaaa_record_store[top]=top_set;
        }
    else{
        dn_aaaa_record_store[top] = set(a);
    }

}
```

```
}


# Input: HTTP Reply information
# Output : Log entries optionally containing abnormal event information
# Read Bro documentation for what fields are in connection record
event http_reply(c:connection, version:string, code:count, reason:string) {
    if (c$http?$host) {
        local subdomains = split_string(c$http$host, /\./);
        # Check to make sure none of the subdomains are whitelisted
        if (!whitelist_domain_check(subdomains)) {
        # Event ID 12 - HIGH NUMBER OF SUBDOMAINS
            local domain_not_ip_check = match_pattern(subdomains[|subdomains|-1], /[a-zA-Z]+/);
            # If more than three subdomains and check to make sure it is a domain, not an IP address
            if (|subdomains| > 3 && domain_not_ip_check$matched){
                push_ab_http_log(c, 12, "High number of subdomains", c$http$host);
            }
        }
    }
}

# Input: HTTP Request information
# Output : Log entries optionally containing abnormal event information
# Read Bro documentation for what fields exist in connection record
event http_request(c: connection, method: string, original_URI: string, unescaped_URI: string, version: string) {
    local base64_uri_query = find_last(unescaped_URI, base64_query_pattern);
    #EVENT ID 09 - BASE64 QUERY STRING
    # If the previous regexp search found a match
    if (base64_uri_query != "") {
        push_ab_http_log(c, 9,"Base64 query string", unescaped_URI);
    }
    #EVENT ID 08 - POST/GET ASYMMETRY
    local host_rec: Host_Rec;
    if(c$id$resp_h in method_freq_map) host_rec = method_freq_map[c$id$resp_h];
    else host_rec = Host_Rec($post_count = 0, $get_count = 0, $other_count=0);
    if(method == "POST") host_rec$post_count += 1;
    else if(method == "GET") host_rec$get_count += 1;
    else{
        host_rec$other_count+=1;
        #EVENT ID 07 - Unknown_HTTP_method
        if( method !in legal_http_methods)
```

```
            # If more than three subdomains and check to make sure it is a domain, not an IP address
            if (|subdomains| > 3 && domain_not_ip_check$matched){
                push_ab_http_log(c, 12, "High number of subdomains", c$http$host);
            }
        }
    }
}

# Input: HTTP Request information
# Output : Log entries optionally containing abnormal event information
# Read Bro documentation for what fields exist in connection record
event http_request(c: connection, method: string, original_URI: string, unescaped_URI: string, version: string) {
    local base64_uri_query = find_last(unescaped_URI, base64_query_pattern);
    #EVENT ID 09 - BASE64 QUERY STRING
    # If the previous regexp search found a match
    if (base64_uri_query != "") {
        push_ab_http_log(c, 9,"Base64 query string", unescaped_URI);
    }
    #EVENT ID 08 - POST/GET ASYMMETRY
    local host_rec: Host_Rec;
    if(c$id$resp_h in method_freq_map) host_rec = method_freq_map[c$id$resp_h];
    else host_rec = Host_Rec($post_count = 0, $get_count = 0, $other_count=0);
    if(method == "POST") host_rec$post_count += 1;
    else if(method == "GET") host_rec$get_count += 1;
    else{
        host_rec$other_count+=1;
        #EVENT ID 07 - Unknown_HTTP_method
        if( method !in legal_http_methods)
                push_ab_http_log(c, 7, "Illegal Http Method", unescaped_URI+" "+method);
        }
    if( host_rec$post_count > 0 && (host_rec$get_count / (host_rec$post_count*1.0)) > 20){
                local tot_count = host_rec$post_count + host_rec$get_count;
                if( c$id$resp_h !in whitelist_ips && (tot_count < 100 || tot_count % 100 == 0))
                        push_ab_http_log(c, 8, "POST/GET ASYMMETRY", unescaped_URI+" "+fmt("post's: %s",host_rec$post_count)+" "+fmt("get's: %s",host_rec$get_count));
        }
    method_freq_map[c$id$resp_h] = host_rec;

}


# Initializes Bro script to write log entries to abnormal_http.log file
```

```
10.0.22.11      10.0.22.100     -       -       dnscat.2ae5ff98d46d7870736163656c7a787769636e6b6a00     dnscat.2ae5ff98d46d7870736163656c7a787769636e6b6a00
fe80::a00:27ff:fea4:2484        ff02::fb        PTR     12      _sane-port._tcp.local   -
10.0.22.11      10.0.22.100     -       -       b8f6ffb967666972756f726f6d796467646d787a7900.foo.klim   b8f6ffb967666972756f726f6d796467646d787a7900.foo.klim
10.0.22.11      10.0.22.100     -       -       -       -
10.0.22.11      10.0.22.100     -       -       711e01aa95cc41ecd5676b00105515ee93.foo.klim     TXT 34 f1fb01aa95de59084366ccffffd97abc6c
10.0.22.11      10.0.22.100     -       -       dd2d01aa95bdb2e063052400114fd195e3.foo.klim     cff001aa95c982de868a12ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       734f01aa95a36df440ca7800234005ff4d.foo.klim     31aa01aa957ea60293b5cbffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       849601aa95947a1261a331000a2562c525.foo.klim     0f7201aa95f1fc01a1c04cffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       59fe01aa952b72a59dd884001566f769c5.foo.klim     6d2101aa959b532c84f705ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       860601aa95c2fa0fa76ac70019a337206b.foo.klim     TXT 34 cfbd01aa95fcd085c3682cffffd97abc6c
10.0.22.11      10.0.22.100     -       -       c97801aa950270e30b83420027e65d202a.foo.klim     01b301aa95cdacbbad67c8ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       bb9c01aa95d163473d257900061cd8b43d.foo.klim     007d01aa95b8f847a0a074ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       4b1901aa958989ee2b967a000b58c01545.foo.klim     2e7701aa95f8eb859228b9ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       106a01aa959dee333614b40014f2ce5fc9.foo.klim     eb5101aa95a07fdafa8622ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       6fd101aa953cfed8b7c35200017c82dda9.foo.klim     591801aa95e5fa08014951ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       544801aa95861b574371dc000ebdd64b56.foo.klim     TXT 34 2cef01aa95ea2c79c52da7ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       ba4b01aa95dd9d796f15980013dd148ba2.foo.klim     edd901aa954914ab6d6ec1ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       ea3001aa95c7154544163000184946d610.foo.klim     9b8f01aa9584b22b4c704afffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       01f101aa95a17bdbd581aa00281b4f792c.foo.klim     8f5501aa953fb3b029b483ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       c50901aa95d3fc17e21ff20003386c9b6a.foo.klim     TXT 34 32f401aa9525d0fa2d9701ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       e26101aa955de3edece1b60012a111f60f.foo.klim     TXT 34 330101aa958d8b1f0957fcffffd97abc6c
10.0.22.11      10.0.22.100     -       -       006601aa9530fd3be0c369002417724ebc.foo.klim     97d001aa9529fbcfd0c9f4ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       747503aa9500000000f64b4de8faed8981a8a858d350154b2653371a095c.02355be519ab89599b54e9641c93cad8bd703ebf99e460b722ae56947b29.ffe27e7e08053c1d8ad4112011.foo.klim
TXT 146 469b03aa9500000000006933e53b9110590102ec319fbcca8c9de27a3b93cfbbfd9232e4c8cfac305c1e31ec2cfb37322f3d00d82ccf3d968eac2ed7077d0b74f1a37f865ed68ce62ef
10.0.22.11      10.0.22.100     -       -       415401aa950401e31e2f2e00098c892cdf.foo.klim     e38301aa95089a9264f65bffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       393401aa958b8df13e546c00268bb510d7.foo.klim     TXT 34 9f8801aa957dd4ef9d6897ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       46b201aa95826bb737455b002d870f50b5.foo.klim     87eb01aa95bc2defa963cefffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       46d301aa951edd1033d95f001d6a8eec41.foo.klim     TXT 34 2e0d01aa95ea2427960643ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       673101aa95b9740b9ba9dc0029d0a86426.foo.klim     0f3501aa955fb664aa3376ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       af6201aa956bdf1b3db0fa002bd3116968.foo.klim     de9501aa9576e861c0840afffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       c34100aa957e9d4bd7575100009b3c22cf435ae19f3a6c5922f9cc210c74.e369963d.foo.klim  TXT 34 859400aa95968aaec54328ffffd97aeedb
10.0.22.11      10.0.22.100     -       -       97af01aa953c5906b1e8360007541af210.foo.klim     ed4d01aa95a9eb5c9251b4ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       07f901aa95ea679253fa69002fdccac48c.foo.klim     202701aa95a92da866652cffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       76e601aa95e2e5e854124e00045360f7e7.foo.klim     4e8201aa952318c268cd06ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       6bb801aa9517f54f5feec0000dc14a8a6c.foo.klim     TXT 34 250f01aa95d0dfc6596be3ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       c79e01aa95ddfc219239a9002e112965fb.foo.klim     e30201aa9584e3e79de5eeffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       e4ed01aa9519b2a387c1ce0030c330ac80.foo.klim     ab5501aa95df62b36f166bffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       941401aa95c344d3d2bb81002caef57cda.foo.klim     b4d901aa95c94a84f9c1f5ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       960801aa9504fdfee2864c000c6108a2d1.foo.klim     af6301aa952bf9fdfb894fffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       6bbc01aa952e6ac23b095900161bea10ec.foo.klim     TXT 34 0d1e01aa95c0908cb96e40ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       4b9501aa95376c2e0365c800178a564962.foo.klim     TXT 34 e59301aa957e7933fc327bffffd97abc6c
10.0.22.11      10.0.22.100     -       -       ae6b01aa95ed692aec8da0001af13cc8ce.foo.klim     675901aa95f9c1dbe633bcffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       074201aa9527102bd09720001c44bdd23c.foo.klim     564c01aa95e70428108f21ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       2ceb01aa9524c62a2cd8490022160e0693.foo.klim     2d9b01aa952c3ae7db80bbffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       806301aa95583d8f10fcbb000f64ae462e.foo.klim     TXT 34 a95c01aa95f53e73b38835ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       56d001aa95a225442743aa002193d0aac5.foo.klim     9c5401aa95b9868d6de82dffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       77cd01aa9565b4ed5e97650002a98e1227.foo.klim     9d5f01aa95f0e8509b6d07ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       b7fb01aa952b074728ef41001b0d6499f8.foo.klim     TXT 34 594c01aa9517121143d1e7ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       e5ea01aa95ab847c5d4282001e5f6f535f.foo.klim     TXT 34 9c4401aa95ad49c11d93b6ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       8fcd01aa95f6dc2a60eecf002544956ed3.foo.klim     713901aa957ec415f93e8dffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       445401aa95a95c6fdeb253002a70f31c14.foo.klim     e4ef01aa9540dd307ef1e7ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       d66801aa9558e13a5c1f810005b0a0c5cc.foo.klim     TXT 34 d99501aa952bc1091bbeb1ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       ccde01aa95cb49dbe23ccd0008fc0cea12.foo.klim     TXT 34 bf2801aa95e3ac1638bc08ffffd97abc6c
10.0.22.11      10.0.22.100     -       -       d1bb01aa951547fd192bfa001f667d8764.foo.klim     57da01aa95f91953003ca5ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       7a1901aa95fc5149cf62ba0020f8a6062f.foo.klim     343601aa956be9b2992793ffffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       40e101aa952b39a8f2c55600316f67111b.foo.klim     82c701aa95e5a6a6a8459effffd97abc6c.foo.klim
10.0.22.11      10.0.22.100     -       -       fc60011f66daa19da36373000114ccb391.foo.klim     TXT 34 bd1c011f662379e929ce38ffff57227a25
10.0.22.11      10.0.22.100     -       -       d4f701aa95c18fa8b7370f004f604629a3.foo.klim     TXT 34 2ce201aa956067d1dcfad9ffffd94cbc1a
```

```
#separator \x09
#set_separator  ,
#empty_field    (empty)
#unset_field    -
#path   weird
#open   2017-09-09-19-08-58
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       name    addl    notice  peer
#types  time    string  addr    port    addr    port    string  string  bool    string
1504956974.972449       CC7bWDiYHfma6Q9G2       10.0.22.11      52129   10.0.22.100     53      bad_UDP_checksum        -       F       bro
1504956974.973038       CC7bWDiYHfma6Q9G2       10.0.22.11      52129   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504957056.903874       -       -       -       -       dns_unmatched_msg       -       F       bro
1504957071.341444       -       -       -       -       dns_unmatched_msg       -       F       bro
1504957102.764208       CXPIh22vqgj7elsw87      10.0.22.11      38290   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504957141.355046       C7BqmY1PKnYfECKCFk      10.0.22.11      58484   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504957195.357924       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504957245.732849       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504957456.045550       -       -       -       -       dns_unmatched_msg       -       F       bro
1504957666.015475       -       -       -       -       dns_unmatched_msg       -       F       bro
1504957797.827782       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504957874.378901       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504958091.384718       -       -       -       -       dns_unmatched_msg       -       F       bro
1504958291.011559       -       -       -       -       dns_unmatched_msg       -       F       bro
1504958400.156477       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504958479.794152       -       -       -       -       dns_unmatched_msg       -       F       bro
1504958499.174737       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504958915.434525       -       -       -       -       dns_unmatched_msg       -       F       bro
1504959001.651425       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504959123.541361       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504959539.951627       -       -       -       -       dns_unmatched_msg       -       F       bro
1504959603.724245       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504959748.150942       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504960139.346389       -       -       -       -       dns_unmatched_msg       -       F       bro
1504960164.276766       -       -       -       -       dns_unmatched_msg       -       F       bro
1504960205.576869       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504960372.320742       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504960527.909766       -       -       -       -       dns_unmatched_msg       -       F       bro
1504960788.469542       -       -       -       -       dns_unmatched_msg       -       F       bro
1504960806.802952       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504960997.104264       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504961408.237398       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504961413.333156       -       -       -       -       dns_unmatched_msg       -       F       bro
1504961621.311683       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504962010.011840       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504962037.532511       -       -       -       -       dns_unmatched_msg       -       F       bro
1504962245.633009       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504962611.296406       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504962662.322187       -       -       -       -       dns_unmatched_msg       -       F       bro
1504962870.525474       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504963213.226171       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
1504963286.697045       -       -       -       -       dns_unmatched_msg       -       F       bro
1504963494.829611       -       -       -       -       dns_unmatched_query_id_quantity -       F       bro
1504963739.240364       -       -       -       -       dns_unmatched_msg       -       F       bro
1504963814.738219       Cf9OBK3DCsSqgnviAd      10.0.22.11      47377   10.0.22.100     53      dns_unmatched_reply     -       F       bro
```


dnsCat.pcap [Wireshar...
Terminal - klim@klim-V...
11 Sep, 13:15
dnsCat.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: dns.qry.type == 0x0010
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
49 2017-09-09 07:40:03.272041 10.0.22.11 10.0.22.100 DNS 103 Standard query 0xff4d TXT ccde01aa95cb49dbe23ccd0008fc0cea12.foo.klim
50 2017-09-09 07:40:03.273275 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0xff4d TXT
61 2017-09-09 07:40:08.325114 10.0.22.11 10.0.22.100 DNS 103 Standard query 0xb20a TXT 6bb801aa9517f54f5feec0000dc14a8a6c.foo.klim
62 2017-09-09 07:40:08.326803 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0xb20a TXT
63 2017-09-09 07:40:09.334464 10.0.22.11 10.0.22.100 DNS 103 Standard query 0xc62c TXT 544801aa95861b574371dc000ebdd64b56.foo.klim
64 2017-09-09 07:40:09.336315 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0xc62c TXT
65 2017-09-09 07:40:10.345197 10.0.22.11 10.0.22.100 DNS 103 Standard query 0x4d19 TXT 806301aa95583d8f10fcbb000f64ae462e.foo.klim
66 2017-09-09 07:40:10.346820 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0x4d19 TXT
67 2017-09-09 07:40:11.355324 10.0.22.11 10.0.22.100 DNS 103 Standard query 0xdd99 TXT 711e01aa95cc41ecd5676b00105515ee93.foo.klim
68 2017-09-09 07:40:11.357203 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0xdd99 TXT
72 2017-09-09 07:40:13.384766 10.0.22.11 10.0.22.100 DNS 103 Standard query 0xd4b5 TXT e26101aa955de3edece1b60012a111f60f.foo.klim
73 2017-09-09 07:40:13.386542 10.0.22.100 10.0.22.11 DNS 150 Standard query response 0xd4b5 TXT
81 2017-09-09 07:40:17.426400 10.0.22.11 10.0.22.100 DNS 103 Standard query 0x2c93 TXT 6bbc01aa952e6ac23b095900161bea10ec.foo.klim
Frame 49: 103 bytes on wire (824 bits), 103 bytes captured (824 bits)
Ethernet II, Src: CadmusCo_a4:24:84 (08:00:27:a4:24:84), Dst: CadmusCo_fd:b7:c9 (08:00:27:fd:b7:c9)
Internet Protocol Version 4, Src: 10.0.22.11 (10.0.22.11), Dst: 10.0.22.100 (10.0.22.100)
User Datagram Protocol, Src Port: 47377 (47377), Dst Port: domain (53)
Domain Name System (query)
[Response In: 801711]
Transaction ID: 0xff4d
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
ccde01aa95cb49dbe23ccd0008fc0cea12.foo.klim: type TXT, class IN
Name: ccde01aa95cb49dbe23ccd0008fc0cea12.foo.klim
Type: TXT (Text strings)
Class: IN (0x0001)
0000 08 00 27 fd b7 c9 08 00 27 a4 24 84 08 00 45 00 ..'..... '.$...E.
0010 00 59 00 00 40 00 40 11 fa 25 0a 00 16 0b 0a 00 .Y..@.@. .%......
0020 16 64 b9 11 00 35 00 45 40 c5 ff 4d 01 00 00 01 .d...5.E @..M....
0030 00 00 00 00 00 00 22 63 63 64 65 30 31 61 61 39 ......"c cde01aa9
0040 35 63 62 34 39 64 62 65 32 33 63 63 64 30 30 30 5cb49dbe 23ccd000
0050 38 66 63 30 63 65 61 31 32 03 66 6f 6f 04 6b 6c 8fc0cea1 2.foo.kl
0060 69 6d 00 00 10 00 01 im.....
Query Type (dns.qry.type), 2 bytes
Packets: 161817 · Displayed: 51528 (31.8%) · Load time: 0:07.322
Profile: Default